# What's Next ?
# Le futur du numérique dans les forces armées

Didier Danet[*], Centre de recherche des écoles de Saint-Cyr Coëtquidan

## Introduction

Le préfixe « Cyber » a incontestablement été l'un des mots clés de l'évolution des forces armées dans la dernière décennie. Dans le monde entier, l'espace numérique est désormais considéré comme un domaine d'exercice de la puissance, de la coercition et de la conflictualité (Taillat 2013) même si les auteurs se partagent sur la nature, les formes ou la probabilité de « guerre » dans l'espace numérique. (Arquilla, Ronfeldt 1992; Rid 2013; Libicki 2012; Kello 2013; Lindsay 2013) Les Etats qui le peuvent reconnaissent explicitement que, au-delà de la protection de leurs systèmes contre les attaques qu'ils pourraient subir (lutte informatique défensive), ils se dotent de capacités de lutte informatique offensive, que celles-ci visent à l'acquisition, la captation ou la falsification d'informations contenues dans des systèmes ennemis, à la détérioration ou la paralysie de dispositifs civils ou militaires par des effets purement cybernétiques ou la combinaison, par exemple, de la lutte informatique et d'actions cinétiques, enfin à la production d'effets visant à peser sur le moral ou les opinions de l'ennemi ou des populations. Les livres blancs sur la Défense et la sécurité affichent la « Cyber défense » comme une priorité à laquelle sont consacrés des moyens budgétaires, humains et techniques très importants (Défense nationale 2013). Des « Cyber Command » sont mis en place (Giles 2011; Samaan 2010; Lynn 2010) et donnent dans certains cas naissance à une « quatrième armée » qui s'émancipe des autres forces attachées à l'espace terrestre, maritime ou aérien. Enfin, des politiques industrielles actives contribuent à soutenir les entreprises susceptibles de développer les innovations requises par la course technologique qui s'est engagée entre les principales puissances mondiales.

[*] Didier Danet est responsable du pôle « Mutation des conflits » du Centre de recherche des écoles de Saint-Cyr Coëtquidan. Il est également directeur du Mastère Spécialisé « Opérations et gestion des crises en cyber défense ».

Cette phase initiale d'émergence et de montée en puissance du numérique dans les rapports de pouvoir et de coercition est désormais acquise. Toute opération militaire comporte une dimension numérique plus ou moins importante. Nul n'ignore que l'espace numérique est l'un de ceux où se jouera le sort des armes et, plus largement, le succès des projets politico-stratégiques. La question qui se pose désormais est celle de l'intégration complète de cette dimension dans l'action globale des forces armées. L'espace numérique n'est pas qu'une source de vulnérabilités et de menaces. Il est tout autant porteur de leviers et d'opportunités qui doivent être exploités au maximum de leurs potentialités, ce qui suppose une articulation délibérée avec les autres dimensions de cette action globale. Le numérique ne se développe pas en parallèle des autres avancées techniques. Il n'est pas isolé au sein d'une structure qui demeurerait insensible à son apparition. Les effets numériques se combinent avec les effets cinétiques, ceux par exemple de la guerre électronique dont ils sont largement indissociables comme l'on montré les opérations menées par la Russie en Ukraine (Pakharenko 2015; Jonsson, Seely 2015) ou en Géorgie (Shakarian 2011; N. 2018). Ils doivent donc être pensés dans le cadre plus large d'une organisation militaire en voie de transformation et d'adaptation à un univers technologique qui a rarement évolué aussi vite.

Un programme en cours de développement dans l'armée de Terre est particulièrement révélateur de cette maturité du numérique dans les forces armées. Il s'agit du programme Scorpion. Ce programme, qui sera rapidement présenté infra, mérite une attention particulière de la part des sciences sociales et politiques car il introduit deux grandes questions relatives à l'équilibre des systèmes socio-techniques et qui sont traditionnellement indissociables de l'appropriation individuelle et collective du progrès technologique ici envisagé sous l'angle particulier du numérique.

La première se pose dès aujourd'hui. La promesse d'efficacité technique de ce système est l'une des plus importantes des programmes d'équipement du dernier quart de siècle. Pour certains, il est possible de parler d'une « ère Scorpion », signe que ce système devrait apporter un avantage majeur aux forces terrestres dans la conduite de leurs missions. Pour autant, l'efficacité d'un système socio-technique ne tient pas seulement à sa dimension technique mais aussi à son appropriation par les individus, les groupes et l'organisation qui le mettent en œuvre. Or, les transformations apportées par le système Scorpion sont suffisamment importantes pour qu'il soit nécessaire de s'interroger sur son efficacité et sur sa résilience organisationnelle lors de sa mise en œuvre dans un environnement hostile.

La seconde question se posera demain. La convergence de nombreuses innovations intervenant dans des champs voisins mais complémentaires fera évoluer Scorpion d'un système socio-technique vers un système techno-social. Autrement dit, les progrès réalisés dans le domaine de l'augmentation des capacités physiques et cognitives des individus (Parasidis 2011; Kotchetkov et al. 2010; Lin, Allhoff 2008) mais aussi l'internet des objets militaires (You, Zhu, Wang 2011; Suri et al. 2016; Zheng, Carter 2015; Yushi, Fei, Hui 2012) ou la robotisation croissante du champ de bataille (Randretsa 2013; Jeangène Vilmer 2015; Doaré, Danet, de Boisboissel 2015) ouvriront deux possibles pour l'évolution des systèmes d'armes. Une première hypothèse est celle de la « machine au service de l'homme », le développement des technologies numériques apportant des aides multiples à la décision et à l'action humaines, depuis les décisions stratégiques des plus hautes autorités militaires jusqu'aux actes élémentaires du combattant sur le terrain. La seconde hypothèse est celle d'une subordination de l'homme aux décisions et aux actions commandées par la machine, l'homme devenant le capteur et l'effecteur d'un système qui est en mesure de décider et d'agir par lui-même. Notre sentiment est que cette seconde hypothèse sera difficilement résistible et que des systèmes comme Scorpion évolueront vers un nouvel équilibre en faveur de la machine sauf à envisager une volonté politique forte du ministère de la Défense pour imposer des mesures de nature à maintenir l'homme actif dans la boucle de l'information et de la décision.

## L'efficacité du numérique au service des forces armées

Le monde militaire est confronté depuis quelques décennies à un défi technologique qui résulte autant de la rapidité du rythme des innovations propres à certains secteurs (notamment celui du numérique) que de la convergence des progrès réalisés par les différentes filières qui alimentent la base industrielle et technologique de la Défense. Pour certains responsables ou analystes américains, cette vague d'innovation doit être maîtrisée par les forces armées des Etats-Unis si celles-ci veulent conserver la supériorité technologique dans le long-terme (Martinage 2014; Fiott 2016; Simón 2016).
Le premier phénomène est le plus évident : les forces armées bénéficient directement de progrès technologiques, souvent réalisés par le monde civil, mais dont le degré de dualité est très élevé et explique leur transfert quasi-immédiat dans le monde militaire. Il suffit pour s'en convaincre de s'intéresser aux innovations disruptives survenues dans la période récente et qui, toutes, ont engendré des applications militaires directes. Le développement des automobiles dites « autonomes » par les entreprises Google ou Uber notamment se retrouve dans de multiples programmes (celui de Lockheed Martin par exemple) qui visent à créer des convois militaires ne nécessitant pas autant de

conducteurs, ressource rare et précieuse, qu'il n'est de camions dans ces convois (Davis et al. 2008; Green 2011). L'automatisation de la machine est également au cœur des réflexions sur les robots terrestres, aériens ou maritimes qui bénéficient aujourd'hui de fonctions de plus en plus accomplies d'aide à la décision ou à l'action. Un système d'armes déjà ancien comme le Phalanx américain offre aux bâtiments de la Marine une protection efficace contre les missiles ennemis qu'il détecte, reconnaît et détruit en ne laissant à l'homme que la possibilité d'interrompre le processus en cas de problème (Wang et al. 2003). Il en va de même des « drones » dont les développements à venir laissent penser qu'ils pourraient demain accompagner les avions de chasse auxquels ils seraient asservis tout en assurant seuls certaines fonctions de reconnaissance ou de protection. Pour ce qui est de son architecture ou de ses principes de fonctionnement, le « Cloud Computing » ne diffère en rien selon qu'il est destiné à des acteurs civils ou à des organisations militaires (Cattaruzza, Danet 2014). On pourrait multiplier les illustrations tirées des différentes filières industrielles : mécanique, électronique, matériaux, énergie… Dans tous ces domaines, les découvertes civiles aboutissent très rapidement à des applications militaires qui ne présentent pas ou peu de différences par rapport aux découvertes d'origine.

Surtout, au-delà de l'application directe d'innovations largement duales, le développement du numérique agit sur les concepts fondamentaux de l'action militaire. Ses progrès bouleversent le temps et l'espace, c'est à dire les cadres les plus structurants de cette action. Ils remettent en cause les données habituelles de la vitesse, de la distance, de la précision et de la connaissance de la situation. Les opérations cybernétiques s'affranchissent des contraintes de temps et de distance ; elles permettent d'atteindre un ennemi lointain de instantanée, voire sans qu'il ne soit en mesure d'identifier l'auteur de l'attaque ni même la nature de cette dernière. La multiplication des capteurs reliés par des réseaux sans fil fournit une masse d'information que le « Big Data » militaire s'efforce de traiter par des processus d'intelligence artificielle, donnant à tous les échelons du commandement une vision inédite du théâtre des opérations. Les perspectives ouvertes par le progrès technique sont telles qu'elles peuvent donner le sentiment que le brouillard et les frictions de la guerre sont en voie d'être surmontés, ce qui serait bien évidemment une illusion mortifère.

S'agissant de l'armée de Terre, la numérisation du champ de bataille prend aujourd'hui la forme particulière d'un programme ambitieux : le programme « Scorpion » (Hémez 2017). Celui-ci vise à moderniser les groupements tactiques interarmes (GTIA) en renouvelant les équipements matériels dont sont dotées les forces (remplacement des véhicules blindés en service actuellement et rénovation du char Leclerc) et en mettant en place un Système d'Information et de Combat

Scorpion (SICS) qui assure la cohérence globale des systèmes mobilisés par l'unification et la modernisation des différents systèmes utilisés jusque là. Dans une première étape, le renouvellement des équipements matériels constitue la partie la plus visible du programme. Le char Leclerc fait ainsi l'objet d'une rénovation importante. Sa protection est renforcée pour tenir compte des menaces apparues sur les théâtres extérieurs, notamment la généralisation des engins explosifs improvisés contre lesquels le Leclerc va bénéficier de kits de blindage spécifiques. Les régiments de cavalerie reçoivent également deux nouveaux véhicules blindés : l'un destiné au transport de troupes (Griffon) et l'autre chargé des missions de combat (Jaguar) En raison de l'importance et du nombre des équipements concernés, cette première phase du programme est donc particulièrement spectaculaire et visible. Pour autant, la deuxième phase du programme, à partir de 2023, nous semble plus significative encore pour l'institution militaire en ce qu'elle touche non seulement à l'équipement matériel des forces mais également à leurs modes d'action, à leurs structures, voire à leur culture professionnelle. La mise en place du SICS offre des possibilités inédites en matière de traitement de l'information, d'aide à la décision et d'action conjointe des différents éléments du GTIA, ce que les documents de doctrine appellent le « combat collaboratif ». Il s'agit pour les différentes composantes du système de partager la connaissance que chacune peut avoir de son environnement immédiat et de la situation tactique, d'accélérer la décision et l'action concertée des acteurs, de réduire le temps de détection d'une menace et de riposte à une attaque… Pour ce faire, les différents équipements qui constituent le système Scorpion profitent d'une vétronique commune : système de contrôle de la navigation, des communications, des systèmes d'observation, de l'énergie et de la motorisation et des systèmes d'armes. Cette capacité inédite du système Scorpion à intégrer horizontalement les unités sur le terrain et verticalement les échelons de décision modifie tout ou presque dans l'action des forces : disposition des unités sur le terrain, gestion des ressources humaines et matérielles en fonction de leurs capacités d'action ou de leur attrition, reconfigurations des unités en cas de pertes, possibilité d'intervention directe des échelons supérieurs dans les décisions opérationnelles... C'est donc bien la numérisation du champ de bataille, plus que l'introduction de nouveaux équipements plus performants, qui induit les transformations les plus substantielles de l'action globale des forces terrestres.

## La question de l'efficacité et de la résilience du système Scorpion

Le système Scorpion peut être considéré, pour l'armée de Terre, comme le système le plus accompli en matière de numérisation du champ de bataille. Mais, on le sait, la performance globale d'un système socio-technique ne dépend pas uniquement de ses capacités techniques intrinsèques ; elle repose tout autant sur des facteurs psycho-sociaux dont l'importance a été mise en évidence par les travaux portant sur le comportement organisationnel (Argyris 1960; Hersey, Blanchard, Johnson 2007; Mohr 1982; Griffin, Moorhead 2011). C'est ce que montre l'application au cas particulier qui est ici traité d'une grille de lecture comme celle de Judge et Robbins qui distingue trois strates possibles d'analyse pour une organisation (Robbins, Judge, Gabilliet 2006).

La première strate est celle de l'individu dont il s'agit de comprendre l'attitude, la personnalité et les valeurs, la motivation... Cette dimension a pris une importance particulière avec la professionnalisation complète des armées et l'impérieuse nécessité pour l'institution d'attirer et de conserver les personnels qui lui sont nécessaires. Les questions liées à la motivation, au moral et à la satisfaction des engagés sont donc essentielles. A cet égard, l'introduction du système Scorpion présente certainement un versant positif. La mise en service de nouveaux véhicules blindés mieux protégés contre les attaques qui se produisent en opérations extérieures ou le déploiement du système Félin qui équipe les fantassins donnent aux engagés l'image d'une armée moderne, bien équipée et entraînée, capable de remplir des missions difficiles en prenant soin de la vie de ses hommes. Cette modernisation joue incontestablement en faveur du moral des troupes. De même, le fait que l'entraînement des forces ait été intégré dans la conception des équipements Scorpion permettra aux utilisateurs de se former directement sur les matériels qu'ils utiliseront sur le terrain, supprimant ainsi l'écart qui peut exister entre les outils de simulation et les équipements opérationnels. Au total, l'appropriation du nouveau système devrait être facilitée par une promesse de performance élevée, un renforcement du sentiment de valorisation et de maîtrise de l'outil et, à tout le moins. Il devrait en résulter une certaine confiance des utilisateurs dans les nouveaux équipements et une absence de frein à la mise en œuvre des équipements (Venkatesh, Thong, Xu 2012; Venkatesh et al. 2003).

La deuxième strate de l'analyse de Judge et Robbins est celle des groupes. Elle est particulièrement centrale dans le cas de l'institution militaire. Les nombreuses études sociologiques qui lui ont été consacrées montrent toutes qu'une large part du succès en mission revient d'abord à la cohésion du groupe restreint, notamment lorsqu'il se trouve dans des environnements fortement hostiles.

Or, à cet égard, l'introduction du système Scorpion est de nature à bouleverser certains des paramètres essentiels de l'action collective. C'est ainsi que la géo localisation permanente des unités et des individus, la multiplication des capteurs permettant de connaître l'état physique et psychologique des combattants ou l'amélioration des communications conduisent à une transformation sensible des modes d'action. Ces innovations permettent notamment d'étirer les distances entre les hommes présents sur le terrain d'où il résulte une plus large occupation du l'espace mais au prix d'un possible sentiment d'isolement et de fragilité. Le commandement « à la voix » qui traduit la proximité des membres de l'unité peut être remplacé par un commandement « à la radio », lequel présente de multiples avantages : clarté des instructions, discrétion… Mais, ce progrès technologique induit une certaine forme d'éloignement du chef de ses subordonnés. Grâce à la multiplication des capteurs de toute nature, le chef militaire dispose d'informations très complètes sur l'état physique et moral de ses troupes. La conduite de la mission peut donc s'appuyer sur une gestion rationnelle des ressources, sur une individualisation fine des efforts et des contraintes mais, ce faisant, cette gestion différenciée risque d'affaiblir le ressort de la solidarité collective et de l'esprit de corps. La construction de cet esprit de corps, la place du chef au sein du groupe, sa manière de commander... sont autant d'éléments clés des comportements organisationnels qui ne manqueront pas d'être affectés au niveau du groupe. L'impact de la numérisation en général et du programme Scorpion en particulier apparaissent tels qu'ils nous semblent appeler à un réexamen des principes fondamentaux du leadership / followership de la part des organismes de doctrine afin de les adapter à ce nouvel environnement marqué par la robotisation et la numérisation du champ de bataille.

Enfin, la troisième strate de l'analyse est celle de l'institution, notamment de la culture qui est la sienne. Ici aussi, le progrès technologique exerce un effet significatif à de nombreux égards.

Il tend, par exemple, à renforcer le caractère technique d'une armée de Terre qui a longtemps été perçue comme moins « savante » que l'armée de l'Air ou la Marine dans lesquelles la maîtrise de systèmes technologiques complexes est profondément inscrite dans la structure et les budgets de l'institution aussi bien que dans la formation et les métiers des personnels (Geistdoerfer 2005; Hamelin 2003). Scorpion constitue un système de systèmes dont la complexité technique et organisationnelle n'a plus rien à envier à ceux des autres armées. Cette évolution n'est pas sans conséquences. S'agissant des hommes, l'armée de Terre constitue une exception par rapport aux autres armées en ce qu'elle est la seule à recruter de manière significative des officiers qui n'ont pas nécessairement une formation d'ingénieur. La numérisation du champ de bataille en général et le programme Scorpion en particulier ne vont pas mettre fin à cette particularité.

Mais, ils sont de nature à modifier l'équilibre actuel à la fois pour ce qui est du ratio des officiers ingénieurs par rapport aux officiers qui ne le sont pas et pour ce qui est de l'image de l'officier de l'armée de Terre. La priorité donnée au recrutement de personnels affectés à la cyber défense tend mécaniquement à renforcer le poids des ingénieurs et des techniciens par rapport à ceux qui ne le sont pas. Il ne s'agit pas d'un véritable bouleversement mais d'une inflexion qui va s'amplifier dans les années à venir. Surtout, cette dimension technique nouvelle peut modifier le « rapport de force » entre les hommes (en termes de carrière par exemple) et en termes d'organisation. Pour ce qui est de l'institution, le poids croissant du numérique devrait donner lieu à de nouveaux rapports de pouvoir entre les armes combattantes et les armes de soutien, en particulier celles qui détiennent l'expertise technique permettant d'assurer la protection des systèmes et la lutte informatique offensive. On peut penser que le caractère relativement ésotérique de domaines comme les architectures de réseaux, l'analyse et le traitement des attaques informatiques ou le chiffrement des données fera très largement de la structure chargée de les concevoir et de les gérer une « boîte noire » pour les non initiés qui devront s'incliner devant les décisions prises par les experts. Les responsables de cette structure pourront arguer de considérations techniques dont ils auront le secret pour donner (ou non) le feu vert à des opérations menées par les forces sur le terrain. Un risque existe de comportements stratégiques de la part d'acteurs ayant compris que leur savoir particulier leur donne une capacité d'influence nouvelle sur les décisions de toute sorte. Sans même aller jusqu'à imputer aux responsables de ces structures un opportunisme débridé, un risque réel d'incompréhension peut résulter du fossé entre ceux qui « parlent cyber » et ceux qui ne le parlent pas. C'est pourquoi, la fonction d'interfaçage et d'intégration du numérique dans les opérations sera centrale dans les opérations futures. Les chefs militaires auront besoin d'intégrer pleinement la dimension numérique dans leurs plans d'opérations. Mais, ils n'accepteront pas de s'en remettre, pieds et poings liés, aux « diktats » qui leur seraient adressés par des experts au nom d'une connaissance qu'ils seraient les seuls à détenir et qu'ils auraient du mal à communiquer en termes accessibles à des non spécialistes. On ne saurait d'ailleurs reprocher à des experts de recourir à des concepts, des méthodes ou des outils adaptés à la complexité du domaine dans lequel ils interviennent et qui sont difficilement « vulgarisables » sauf à perdre en rigueur et en validité.

Il convient donc d'instaurer auprès des chefs militaires des officiers disposant d'une double culture technique (aptitude à comprendre les principes fondamentaux de la technique numérique) et opérationnelle (maîtrise de l'intégration des contraintes et opportunités numériques dans la planification et la conduite des opérations) Sans ce type de profil, les organisations militaires redécouvriront à leurs dépens les charmes de la théorie de l'acteur stratégique de Crozier et Friedberg.

## La place de l'homme dans le système Scorpion

Comme tous les grands équipements militaires, le système Scorpion a vocation à s'inscrire dans la durée et il est donc appelé à évoluer. Il l'est d'autant plus que son « coeur numérique » connaît un rythme d'innovation particulièrement rapide. Deux des évolutions attendues dans les prochaines années sont ainsi de nature non seulement à accroître le niveau de performance global du système mais également à en modifier la nature même et à faire bouger l'équilibre existant entre l'homme et la machine.

A l'heure actuelle, Scorpion est un système socio-technique. Certes, les progrès techniques sont spectaculaires et le niveau d'automatisation de certaines fonctions s'est fortement accru. La coordination des feux en cas d'attaque en est un exemple manifeste. Mais, dans un futur relativement proche, le développement de l'intelligence artificielle appliquée au « Big Data militaire » et celui du « Human Enhancement » ouvriront plusieurs possibles sans qu'il soit encore possible de dire lequel l'emportera.

La multiplication des capteurs produit d'ores et déjà des volumes importants de données de toutes sortes sur les terrains d'intervention, les forces ennemies, l'état des matériels… « L'Internet of Military Things » entraînera très rapidement une croissance exponentielle de ce volume qui ne pourra être utilement traité que par des programmes d'intelligence artificielle (notion de « Big Data militaire ») Ces programmes pourront non seulement exploiter les données recueillies mais également fournir des prédictions quant au comportement des forces adverses et des recommandations en termes d'actions à conduire. Comme nous l'avons vu, la lutte contre les bombes artisanales (Improvised Explosive Devices) est intégrée dans le programme Scorpion à travers le renforcement de la protection des Leclerc et des autres blindés. Mais, le point essentiel de cette lutte réside dans la détection et le désamorçage des IED. Pour ce faire, les forces armées s'en remettent aujourd'hui à la vigilance des responsables de convoi et à l'exploitation des images aériennes fournies par les drones.

Mais, il s'agit d'un travail fastidieux et qui est très coûteux en ressources humaines expérimentées. Les capacités nouvelles du « Machine Learning », notamment la classification d'objets, permettront rapidement d'automatiser cette fonction et de traiter des volumes importants de données dans des délais très réduits, ce qui apportera une sécurité supplémentaire lors des déplacements sur les théâtres extérieurs (Whitney et al. 2009; Jarman et al. 2010). Dans un deuxième temps, il est possible d'imaginer des intelligences artificielles plus évoluées, capables de combiner données techniques et données comportementales afin non seulement de détecter les menaces existantes mais aussi d'anticiper les scénarios d'attaques (Whitney, Brother). De manière générale, la croissance du volume des données captées par les systèmes militaires impose l'automatisation très large de son traitement et l'intégration des résultats obtenus dans les processus de décision.

Le « Human Enhancement » peut se définir comme l'intervention sur le corps humain afin d'en accroître les possibilités physiques ou cognitives en allant au-delà des capacités « naturelles » de l'individu (Letonturier 2014; Dorlhiac 2016; Claverie 2010). Il procède de la convergence des progrès réalisés dans les domaines de la médecine, de la biologie, des matériaux ou des technologies numériques. Les liens entre « Human Enhancement » et technologies du numérique sont appelés à connaître un développement privilégié. C'est ainsi que le développement des interfaces neuronales directes va permettre au cerveau humain de communiquer avec la machine sans passer par l'intermédiaire d'interfaces telles que la parole ou le clavier (Graimann, Allison, Pfurtscheller 2009; Schalk et al. 2004). Ces interfaces réalisent donc une extension du domaine du numérique, faisant de l'homme, non plus seulement l'utilisateur d'un système auquel il reste extérieur, mais un composant à part entière de ce système, capable de l'alimenter en données et de recevoir en retour les éléments qui lui permettent de prendre des décisions ou d'agir en meilleure connaissance de cause. Cette imbrication poussée de l'homme et du système numérique peut se concevoir de deux manières.

La première est celle d'une démultiplication des potentialités humaines par l'apport de capacités de mémorisation, d'analyse ou d'aide à la décision considérablement amplifiées. Le combattant transfère au SICS les données internes (état de fatigue, stress…), celles relatives à son équipement (niveau de munition, autonomie énergétique…) et à son environnement (position, obstacles…) et reçoit en retour une information synthétique sur le niveau de danger, la progression des autres membres de l'unité, les mouvements à opérer ou les indications de tir… Muni de ces aides à la décision et à l'action, le combattant gagne en autonomie et en sécurité. Il peut mener sa mission à bien en s'appuyant sur les possibilités nouvelles offertes par l'intégration du numérique dans l'action globale des forces armées. C'est le sens d'un programme comme le « Urban Leader Tactical

Response, Awareness and Visualization » mené par la DARPA et dont l'une des applications les plus connues est un dispositif d'affichage tête haute qui permet au soldat de recevoir les images produites par un drone, d'afficher la carte des environs ou de faire apparaître les « points d'intérêt » grâce à la réalité augmentée (Livingston et al. 2011; Ai, Livingston, Decker 2011; Ai, Livingston 2009). Dans cette hypothèse, l'homme reste bien au coeur des opérations mais il bénéficie de l'assistance que le développement des outils numériques et bio-médicaux peut lui procurer en matière d'information, de décision et d'action. Il n'y a pas de rupture par rapport à la situation actuelle et le progrès conduit à un développement linéaire du degré d'automatisation de certaines fonctions (information, communication, aide à la décision…) ce qui soulage le combattant et lui permet de se concentrer sur les tâches essentielles de la mission sans le priver des responsabilités qui sont les siennes. L'imbrication plus poussée de l'homme et de la machine, permise par le développement des IND, se traduit alors par un enrichissement du métier militaire et une forme de rationalisation de l'action collective.

La deuxième conception possible du rapport homme / machine dans un système tel que le Scorpion est celle d'une subordination croissante du premier à la seconde, l'homme devenant une sorte de capteur / effecteur dont l'intérêt serait principalement de suppléer le robot dans les situations où l'usage de celui-ci n'est pas possible ou opportun. De nombreuses raisons techniques peuvent pousser à cette deuxième hypothèse. Lorsque la machine est substituable à l'homme, elle présente des qualités essentielles pour l'action militaire : elle est plus rapide et plus précise, ne se laisse pas envahir par les émotions, ne subit pas les effets négatifs de l'ennui ou de la routine… Dans le combat collaboratif, le feu coordonné de trois engins blindés sera plus efficace s'il est piloté par le programme de détection et de riposte une fois que celui-ci a été activé par l'autorité compétente plutôt que si ce feu est contrôlé par les équipages eux-mêmes. Dans ces hypothèses, l'officier ou le soldat sont considérés comme les « maillons faibles » du dispositif techno-social : hétérogènes, lents, disposant de capacités cognitives limitées et d'une mémoire faillible, d'une rationalité limitée…, ils ont vocation à être guidés par la machine, voire remplacés par elle lorsqu'elle le peut. La limite serait alors que l'homme reste supérieur à la machine pour un certain nombre de tâches ou dans un certain nombre de situations. Le milieu terrestre est par exemple plus compliqué que les milieux aériens ou marins pour l'orientation et les déplacements des robots et l'homme peut donc conserver un avantage comparatif. Mais, si le soldat humain est alors utilisé pour ses capacités de franchissement, la machine « reprend la main » dès qu'elle le peut, par exemple pour décider du chemin à suivre ou pour réaliser une action où elle guide le bras de l'homme (un tir de précision par exemple).

A supposer que l'homme ne soit pas purement et simplement soumis à une intelligence artificielle qui décidera pour lui et le guide dans son action, la tentation n'en sera pas moins grande de faire remonter la prise de décision et le pilotage de l'action opérationnelle vers les échelons supérieurs du commandement. Grâce à la puissance du système d'information, l'Etat-Major disposera tout à la fois d'une vue d'ensemble de la situation politico-militaire et des données élémentaires de chaque unité sur le terrain. Le Général en chef pourra se muer à tout instant en chef de section et court-circuiter la ligne hiérarchique.

Au total, c'est donc la question de la place, de l'autonomie et du statut des différents acteurs de la chaîne hiérarchique qui se trouve posée du fait des progrès attendus de la numérisation du champ de bataille et de l'intégration de plus en plus poussée de la dimension numérique dans l'action globale des forces armées.

## Conclusion

Après avoir assez largement envahi l'espace des relations internationales et de la conflictualité, quel peut être l'avenir du « Cyber » pour les forces armées ?

Un premier pari peut être tenté, celui de la fin d'une époque marquée par les dystopies techno-apocalyptiques. Dans la période que l'on pourrait qualifier d'émergence et de montée en puissance du discours sur la « Cyberwar », celui-ci a largement privilégié un discours de la peur et mis en avant la menace d'un « Cyber Pearl Harbor », c'est à dire d'une attaque informatique contre des infrastructures critiques (énergie, transport, système bancaire…) dont la paralysie ou la destruction serait susceptible d'engendrer le chaos économique et social, voire des accidents catastrophiques et des pertes humaines spectaculaires (Valentin 2010; Wilson 2003; Molfino 2016). Ce discours alarmiste a conduit à une vision particulière de la « Cyber Défense », d'abord conçue comme une lutte défensive, centrée sur la sécurité des systèmes d'information. Il s'est souvent agi de faire de ces systèmes des châteaux-forts numériques en les entourant de couches protectrices toujours plus nombreuses et de murs toujours plus hauts (Jajodia et al. 2011; Kuipers, Fabro 2006; Lippmann et al. 2006). Incontestablement utile et nécessaire, le durcissement des systèmes d'information contre les attaques de plus en plus nombreuses et de plus en plus sophistiquées présente des faiblesses évidentes et appelle à un renouvellement du modèle lui-même comme le suggère fort pertinemment Christian Leuprecht (Leuprecht, Skillicorn, Tait 2016). Surtout, cette approche défensive et technicienne n'épuise par la question du « Cyber » pour les forces armées. Celles-ci sont engagées dans un processus plus vaste de déploiement de leur action dans un espace conflictuel, à la fois

physique et numérique, processus qui est moins technique que socio-politique, plus centré sur l'utilisation de l'outil que sur ses recettes de fabrication, soucieux d'une pleine insertion de la dimension « cyber » dans la stratégie générale de l'institution et d'une combinaison de ses effets avec ceux des autres armes (Cattaruzza, Danet, Taillat 2018). En bref, le numérique n'est plus un champ entièrement à part de l'activité des forces armées mais un vecteur d'intégration à part entière de l'action globale qu'elles visent à mettre en oeuvre. Le « Cyber », fin en soi, cède la place au « numérique », vecteur de transformation des structures et des modalités de l'action coercitive.

La fascination pour les aspects techniques est en voie de dissipation. Le mythe du « bidouilleur de génie », isolé mais capable de défier et de mettre à mal les institutions étatiques les plus puissantes est en voie de dissipation. L'espace numérique n'est pas celui de l'asymétrie radicale et les services étatiques le dominent très largement (Taillat 2016). L'anonymat tend à en disparaître du fait des progrès du « Forensics » et des lois de surveillance. Aucun « Cyber Pearl Harbor » ne s'est produit en dépit des attaques répétées contre les infrastructures critiques (Smith 1998; Dunn Cavelty 2013; Desforges 2014). Une opération aussi sophistiquée que Stuxnet, manifestement conçue et mise en oeuvre par les acteurs étatiques les plus avancés, a détruit certaines centrifugeuses iraniennes mais n'a finalement guère entamé la capacité du pays à développer son programme nucléaire (Barzashka 2013; Lindsay 2013). En bref, l'illusion d'une arme cybernétique toute puissante a fait long feu. Tout comme dans d'autres domaines où la technique est particulièrement prégnante (le nucléaire par exemple), les considérations politiques et stratégiques tendent à retrouver leur primauté, la finalité politique et militaire ayant vocation à l'emporter sur la technique mise en oeuvre.

La question centrale qui se pose aujourd'hui au « numérique » est celle de sa contribution possible à une action globale au service d'un projet politique. Il s'agit donc de l'envisager pour son aptitude à préserver la liberté d'action des forces, notamment par l'indispensable protection des systèmes d'information et de commandement, et à produire des effets sur le champ de bataille (espionnage, sabotage, influence…) A cet égard, l'action numérique ne saurait être envisagée indépendamment ou isolément des autres formes d'action des forces armées. Elle constitue l'une des dimensions de la stratégie globale et elle doit y être pleinement intégrée à travers le processus de planification et de conduite des opérations. L'avenir du numérique au sein des forces armées devrait donc être placé sous le signe d'une progressive banalisation. Deux points de vigilance nous semblent devoir s'imposer à cet égard.

La première menace consisterait dans une exacerbation des comportements stratégiques de la part des structures chargées de la cyber défense qui profiteraient de la complexité technique du domaine pour s'ériger en « boîte noire » et restreindre la capacité des chefs militaires à décider en pleine connaissance de cause et responsabilité. La formation et le déploiement d'officiers chargés d'assurer l'interface entre les structures techniques et les organismes de commandement apparaît essentielle pour prévenir cette menace. Ils devront disposer de compétences techniques suffisantes pour prendre la mesure des difficultés rencontrées et des solutions à adopter et de compétences en matière de planification et de conduite des opérations, voire de gestion de crises, pour donner sa juste place à la dimension cyber dans la conception et le déroulement de la manoeuvre globale.

La seconde serait celle du déni, c'est à dire du refus de comprendre que la numérisation dépasse de cent coudées la seule dimension technique et qu'elle affecte l'ensemble de l'institution dont elle invite à repenser certains équilibres fondamentaux. Celle-ci ne doit pas hésiter à tirer toutes les conséquences que peut avoir sur les individus, les groupes et l'organisation l'évolution particulièrement forte et rapide qui caractérise le numérique. Dès aujourd'hui, on ne peut sans doute plus organiser les unités, commander les hommes ou conduire une mission comme on le faisait au XX° siècle. Sans cette réflexion sur les structures, les concepts ou la doctrine, l'intégration du numérique sera incomplète et elle ne permettra pas de poser explicitement la question de l'intégration du numérique dans la conflictualité contemporaine.

## Bibliographie

Ai, Zhuming, Livingston, Mark A. Et Decker, Jonathan W., 2011. *Mission Specific Embedded Training Using Mixed Reality*. Naval Research Lab Washington Dc.

Ai, Zhuming Et Livingston, Mark A., 2009. "Integration Of Georegistered Information On A Virtual Globe". In : *Mixed And Augmented Reality, 2009. Ismar 2009. 8th Ieee International Symposium On*. Ieee. 2009. Pp. 169–170.

Argyris, Chris, 1960. *Understanding Organizational Behavior*. . 1960.

Arquilla, John Et Ronfeldt, David F, 1992. *Cyberwar Is Coming!* Santa Monica, Calif. : Rand.

Barzashka, Ivanka, 2013. "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact On The Iranian Enrichment Programme". *The Rusi Journal*. 2013. Vol. 158, N° 2, Pp. 48–56.

Cattaruzza, Amaël, Danet, Didier et Taillat, Stéphane, 2018. *Cyber Défense*. Paris : Armand Colin. Collection U.

Cattaruzza, Amaël Et Danet, Didier, 2014. "Cloud Souverain Et Balkanisation Du Web : Le Cas Des Etats-Unis". In : *La Balkanisation Du Web*. Ministère De La Défense. Paris : Frédérick Douzet.

Claverie, Bernard, 2010. *L'homme Augmenté*. L'Harmattan.

Danet, Didier, Doare, Ronan et De Boisboissel, Gérard, 2015. *Drones Et « Killer Robots » : Faut-Il Les Interdire ?*, Presses Universitaires de Rennes. Rennes. L'univers des normes.

Davis, James, Animashaun, Asisat, Schoenherr, Edward et Mcdowell, Kaleb, 2008. "Evaluation Of Semi-Autonomous Convoy Driving", *Journal Of Field Robotics*. 2008. Vol. 25, N° 11-12, Pp. 880–897.

France, Commission Du Livre Blanc Sur La Défense et la sécurité nationale, 2013. *Livre Blanc (Le)*. La Documentation Française.

Desforges, Alix, 2014, "Les représentations du cyberespace: un outil géopolitique", *Hérodote*. 2014. n° 1, pp. 67–81.

Doaré, Ronan, Danet, Didier Et De Boisboissel, Gérard, 2015. *Drones et Killer Robots : faut-il les interdire?* Presses Univ. De Rennes.

Dorlhiac, Sébastien, 2016, "Le futur du soldat sur le champ de bataille : le robot?", *Stratégique*. 2016. n° 2, p. 125–144.

Dunn Cavelty, Myriam, 2013, "Un cyber Pearl Harbor : quelle probabilité a court terme ?" *Défense Sécurité Internationale (Dsi)*, 2013. Numéro Spécial, N° 32, Pp. 30-32.

Fiott, Daniel, 2016, "Europe And The Pentagon's Third Offset Strategy", *The Rusi Journal*, 2016, Vol. 161, n° 1, p. 26–31.

Geistdoerfer, Patrick, 2005, La formation des officiers de marine: de Richelieu au XXIème siècle, des gardes aux "bordaches", *Techniques Et Culture*, 2005, n° 45, p.6

Giles, Keir, 2011, "'Information Troops" - A Russian Cyber Command?", 2011 3rd International Conference On Cyber Conflict (Ieee), 2011, p.1–16

Graimann, Bernhard, Allison, Brendan Et Pfurtscheller, Gert, 2009, "Brain–Computer Interfaces: A Gentle Introduction", *Brain-Computer Interfaces*, Springer, p. 1–27

Green, Damian A., 2011, *Future Of Autonomous Ground Logistics: Convoys In The Department Of Defense*. Army Command And General Staff Coll Fort Leavenworth Ks School Of Advanced Military Studies.

Griffin, Ricky W. Et Moorhead, Gregory, 2011, *Organizational Behavior*, Cengage Learning.

Hamelin, Fabrice, 2003, "Le combattant et le technocrate. La formation des officiers a l'aune du modèle des élites civiles", *Revue française de science politique*, 2003, vol. 53, n° 3, p. 435–463.

Hémez, Rémy, 2017, "The French Army At A Crossroads", *Parameters*, 2017, vol. 47, n° 1, p. 103.

Hersey, Paul, Blanchard, Kenneth H. Et Johnson, Dewey E., 2007, *Management Of Organizational Behavior*, Prentice Hall Upper Saddle River, Nj.

Jajodia, Sushil, Noel, Steven, Kalapa, Pramod, Albanese, Massimiliano Et Williams, John, 2011, "Cauldron Mission-Centric Cyber Situational Awareness With Defense In Depth", *Military Communications Conference, 2011-Milcom 2011*, IEEE, p. 1339–1344

Jarman, Kenneth D., Brothers, Alan J., Whitney, Paul D., Young, Jonathan Et Niesen, David A., 2010, *Integrating System Dynamics And Bayesian Networks With Application To Counter-Ied Scenarios*, Pacific Northwest National Laboratory (Pnnl), Richland, Wa (Us).

Jeangène Vilmer, Jean-Baptiste, 2015, "Drones armés et systèmes d'armes létaux autonomes : des enjeux différents", *Drones Et Killer Robots: faut-il les interdire?* Presses Universitaires De Rennes. p. 91-102.

Jonsson, Oscar Et Seely, Robert, 2015, "Russian Full-Spectrum Conflict: An Appraisal After Ukraine", *The Journal Of Slavic Military Studies*. vol. 28, n° 1, p. 1–22.

Kello, Lucas, 2013, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft",

*International Security*, vol. 38, n° 2, p. 7–40.

Kotchetkov, Ivan S., Hwang, Brian Y., Appelboom, Geoffrey, Kellner, Christopher P. Et Connolly Jr, E. Sander, 2010, "Brain-Computer Interfaces: Military, Neurosurgical, and Ethical Perspective", *Neurosurgical Focus*, vol. 28, n° 5, p. E25.

Kuipers, David Et Fabro, Mark, 2006, *Control Systems Cyber Security: Defense In Depth Strategies*, Idaho National Laboratory (Inl).

Letonturier, Eric, 2014, "Au-delà du «soldat-robot»: l'éthique comme augmentation", *Hermès, La Revue*, n° 1, p. 139–142.

Leuprecht, Christian, Skillicorn, David B. Et Tait, Victoria E., 2016, "Beyond The Castle Model Of Cyber-Risk And Cyber-Security", *Government Information Quarterly*, vol. 33, n° 2, p. 250–257.

Libicki, Martin C., 2012, *Crisis And Escalation In Cyberspace*, Rand Corporation.

Lin, Patrick et Allhoff, Fritz, 2008, "Untangling The Debate: The Ethics Of Human Enhancement", *Nanoethics*, vol. 2, n° 3, p. 251.

Lindsay, Jon R., 2013, "Stuxnet and The Limits of Cyber Warfare", *Security Studies*, vol. 22, n° 3, p. 365–404.

Lippmann, Richard, Ingols, Kyle, Scott, Chris, Piwowarski, Keith, Kratkiewicz, Kendra, Artz, Mike et Cunningham, Robert, 2006, "Validating And Restoring Defense In Depth Using Attack Graphs", *Military Communications Conference,* MILCOM, IEEE, p. 1–10.

Livingston, Mark A., Rosenblum, Lawrence J., Brown, Dennis G., Schmidt, Gregory S., Julier, Simon J., Baillot, Yohan, Swan, J. Edward, Ai, Zhuming Et Maassel, Paul, 2011, "Military Applications Of Augmented Reality", in *Handbook Of Augmented Reality*, Springer, p. 671–706.

Lynn, William J., 2010, "Defending A New Domain: The Pentagon's Cyberstrategy", *Foreign Affairs*. vol. 89, n° 5, p. 97–108.

Martinage, Robert, 2014. *5oward A New Offset Strategy: Exploiting Us Long-Term Advantages To Restore Us Global Power Projection Capability*. Center For Strategic And Budgetary Assessments,.

Mohr, Lawrence B., 1982. *Explaining Organizational Behavior*. Jossey-Bass.

Molfino, Emily, 2016, "Cyberterrorism: Cyber "Pearl Harbor" Is Imminent", in *Cyberspaces And Global Affairs*, Routledge, p. 101–108.

N., Anthony, 2018, "Les opérations numériques dans les conflits contemporains", in *Cyberdéfense*, Paris, Armand Colin, Collection U, Amaël Cattaruzza, Stéphanetaillat Et Didier Danet (Ed).

Pakharenko, Glib, 2015, "Cyber Operations At Maidan: A First-Hand Account", in *Cyber War In Perspective: Russian Aggression Against Ukraine*, Kenneth Geers, Tallinn, 2015, p. 59–66.

Parasidis, Efthimios, 2011, "Human Enhancement And Experimental Research In The Military", *Conn. L. Rev.* 2011, vol. 44, p. 1117.

Randretsa, Thierry, 2013, "L'autonomisation des robots sur le champ de bataille. la guerre, le droit et l'éthique", *Revue Internationale Et Stratégique*, 2013, n° 4, p. 18–27.

Rid, Thomas, 2013, *Cyber War Will Not Take Place*, Oxford University Press.

Robbins, S. P, Judge, T. et Gabilliet, P., 2006, *Comportements Organisationnels*, 12° édition, Pearson Education.

Samaan, Jean-Loup, 2010, "Cyber Command: The Rift In Us Military Cyber-Strategy", *The Rusi Journal*, 2010, vol. 155, n° 6, p. 16–21.

Schalk, Gerwin, Mcfarland, Dennis J., Hinterberger, Thilo, Birbaumer, Niels Et Wolpaw, Jonathan R., 2004, "Bci2000: A General-Purpose Brain-Computer Interface (Bci) System", in IEEE

*Transactions On Biomedical Engineering*, 2004, vol. 51, n° 6, p. 1034–1043.

Shakarian, Paulo, 2011, "The 2008 Russian Cyber Campaign Against Georgia", *Military Review*, 2011, vol. 91, n° 6, p. 63.

Simón, Luis, 2016, "The 'Third'us Offset Strategy And Europe's 'Anti-Access' Challenge", *Journal Of Strategic Studies*, 2016, vol. 39, n° 3, p. 417–445.

Smith, George, 1998, "An Electronic Pearl Harbor? Not Likely", *Issues In Science And Technology*, 1998, vol. 15, n° 1, p. 68–73.

Suri, Niranjan, Tortonesi, Mauro, Michaelis, James, Budulas, Peter, Benincasa, Giacomo, Russell, Stephen, Stefanelli, Cesare Et Winkler, Robert, 2016, "Analyzing The Applicability Of Internet Of Things To The Battlefield Environment", 2016 International Conference On Military Communications And Information Systems (Icmcis), IEEE, p. 1–8.

Taillat, Stéphane, 2013, "Le cyberespace, un nouveau domaine de la guerre ?" in *Les Frontières Du Cyberespace*, Ecole des Transmissions, Rennes.

Taillat, Stéphane, 2016, "Un mode de guerre hybride dissymétrique? Le cyberespace", *Stratégique*, n° 1, p. 89–106.

Valentin, Jean-Michel, 2010, "Le syndrome Pearl Harbor et les fables de la technologie", 1986-2000. *Frontières*, p. 93-110.

Venkatesh, Viswanath, Morris, Michael G., Davis, Gordon B. Et Davis, Fred D., 2003, "User Acceptance Of Information Technology: Toward A Unified View", *Mis Quarterly*, p. 425–478.

Venkatesh, Viswanath, Thong, James Yl Et Xu, Xin, 2012, "Consumer Acceptance And Use Of Information Technology: Extending The Unified Theory Of Acceptance And Use Of Technology", *Mis Quarterly*, p. 157–178.

Vilmer, Jean-Baptiste Jeangène, 2013, "Introduction: Robotisation Et Transformations De La Guerre", *Politique étrangère*, n° 3, p. 80–89.

Wang, Shao-Gang, Li, Qun, Liu, Chen Et Zhu, Yi-Fan, 2003, "Modeling And Simulation Of The Weapon System Of Phalanx", *Computer Simulation*, vol. 11, p.6.

Whitney, Paul, Brothers, Alan, Coles, Garill, Young, Jonathan, Wolf, Katherine, Thompson, Sandy, Niesen, David, Madsen, John Et Henderson, Cindy, 2009, "Technosocial Modeling Of Ied Threat Scenarios And Attack", in *Aaai Spring Symposium: Technosocial Predictive Analytics*, op. 142–147.

Wilson, Clay, 2003, "Computer Attack And Cyber Terrorism: Vulnerabilities And Policy Issues For Congress", *Focus On Terrorism*, vol. 9, p. 1–42.

You, Chun-Yan, Zhu, Gui-Bin Et Wang, Yang, 2011, "The Internet Of Things And Its Military Applications", *Journal Of Military Communications Technology*, vol. 1, p. 16.

Yushi, Lan, Fei, Jiang Et Hui, Yu, 2012, "Study On Application Modes Of Military Internet Of Things (Miot)", *2012 Ieee International Conference On Computer Science And Automation Engineering (Csae),* IEEE, p. 630–634.

Zheng, Denise E. Et Carter, William A., 2015, *Leveraging The Internet Of Things For A More Efficient And Effective Military*, Rowman & Littlefield.