Les évolutions du paradigme cyber

Antony Dabila

Titre revue : Revue de défense nationale, numéro 806
Date de publication : 2018

Les évolutions du paradigme cyber: de la « 4e armée» à l'intégration cybertactique

Par ***Antony Dabila***

À mesure que les menaces issues de l'informatisation de nos sociétés deviennent plus concrètes en faisant irruption dans notre quotidien et dans les pages internationales de nos journaux, les défis numériques auxquels les armées devront faire face deviennent plus tangibles. Auparavant difficile à prévoir, l'utilisation des nouvelles technologies *à l'intérieur de l'espace de bataille* s'est grandement précisée au cours des dernières années[1]. Nous avons en effet été témoins de conflits menés par des groupes insurrectionnels sous-financés, ayant dû mettre en place de nouvelles formes stratégiques et tactiques pour lutter contre leurs ennemis, en l'absence de corps doctrinal bien établi et de modèle étatique d'armée de masse appuyée sur des équipements lourds[2].

Leur détermination à profiter de tous les bénéfices des nouvelles technologies de communication bon marché pour faire le maximum de dégâts avec le minimum de budget se place dans la droite ligne stratégique de l'*Appel à la résistance islamique mondiale* publié en 2004 par le stratège d'Al-Qaïda Abu Musab al-Suri[3]. En particulier, la guerre en Syrie-Irak a aussi permis d'observer les conséquences opérationnelles d'une généralisation du recours aux moyens numériques, dont un grand nombre de domaines (communication, reconnaissance, renseignement, propagande, recrutement, revendication, etc.).

La question de la numérisation de l'outil militaire est ainsi venue se placer au cœur du débat de politique de défense hexagonal. Une solution en vogue voudrait que, pour répondre à une menace dans un « nouvel espace », nous créions une « 4e armée », dévolue aux tâches de cybersécurité. Ce serait le chemin le plus direct pour assurer notre protection numérique, dans la droite ligne de l'idée de « continuum sécurité-défense ». Cette proposition figurait au programme de deux des principaux candidats à l'élection présidentielle[4]. Fondée sur le principe mahanien « à chaque domaine [géographique] de la guerre son armée », elle n'est pas satisfaisante. Il n'est pas possible de comparer strictement le domaine aérien ou marin au « cyberespace ». Les deux premiers sont des milieux géographiques imposant un système technique permettant d'y évoluer, tandis que le « milieu » informatique est un « ensemble technique »[5] entièrement nouveau s'adaptant à tous les espaces géographiques. C'est d'ailleurs un autre modèle, « l'intégration cyber-tactique »[6], vers lequel la France semble s'orienter. Nous examinerons la nature du défi auquel sont confrontées les forces françaises, puis la teneur des solutions déjà fournies et celles prodiguées dans la Revue Stratégique, pour tenter de comprendre quels sont les réels enjeux de ce débat.

---

[1] *Strategic Cyberspace Operations Guide*, United States Army War College, Carlisle, Pennsylvania, juin 2016, p.9.
[2] Pour une analyse pertinente des effets, voir Joseph Henrotin, *Techno-guérilla et guerre hybride, le pire des deux mondes*, Paris, Nuvis, 2014
[3] Brynjar Lia, *Architect of global Jihad*, London & New York, Hurst &Columbia University Press, 2008.
[4] À savoir François Fillon (voir la page 14 de son programme "Pour Vous"), Emmanuel Macron, par l'entremise de son actuel Secrétaire d'État chargé du numérique, M. Mahjoub (http://www.numerama.com/politique/258670-mounir-mahjoubi-appelle-a-la-creation-dune-cyber-armee-qui-existe-deja.html). C'était déjà la position de J.-Y. Le Drian lors du précédent quinquennat (http://www.leparisien.fr/high-tech/le-drian-souligne-le-role-essentiel-de-la-cyberdefense-06-10-2014-4192305.php).
[5] Au sens de Gilbert Simondon.
[6] Concept que nous développons à partir du *Strategic Cyberspace Operations Guide* et de sa "*cross-domain integration*"

I) Mise à jour du système de communication et de coordination requise

L'hypothèse soutenue dans cet article sera simple : le trop grand usage des mots composés à partir du préfixe cyber- (cyberguerre, cyberespace, cybersécurité, cybermenace, etc.) a conduit à une dilatation préjudiciable du concept[7]. Elle empêche en effet les forces armées de se concentrer sur leur mission première, qui est *l'intégration cyber-tactique*, c'est-à-dire l'importation de tous les nouveaux dispositifs de communications et d'analyse numériques aux fonctions de combat et de commandement[8], aboutissant à l'établissement d'un « système de communication et de coordination » entièrement nouveau.

Pour être efficaces, ces systèmes ne doivent pas seulement suivre une logique technique qui en ferait un outil inadapté aux utilisateurs, à savoir les militaires. Un des principaux défis de la réussite de son implantation réside donc dans sa cohérence avec le modèle d'armée sur lequel cet « ensemble technique » est greffé. Il n'existe par conséquent pas « un » modèle unique à suivre, mais une multiplicité de solutions dont la meilleure sera celle qui permettra aux armées d'améliorer le plus possible ses fonctions de combat, tout en faisant apparaître le moins de vulnérabilités numériques possible[9].

Or, la volonté de donner à la « cybermenace »[10] un caractère global et, par conséquent, de charger l'armée de lutter contre l'ensemble des dangers pouvant surgir du « cyberespace » ne va pas sans inconvénient. Elle constitue sûrement une stratégie d'argumentation pertinente pour convaincre les hiérarchies en place dans l'armée de faire une place aux nouvelles technologies, qui ont pu paraître à leur début comme de simples « gadgets » face aux véritables armes de guerre. Cette manière de présenter a pu aussi être utile, à l'intérieur du jeu de bureaucraties en concurrence pour voir augmenter sa part du budget étatique, en insistant sur l'idée de « nouvelles menaces » auprès des décideurs politiques et de l'opinion publique.

Malgré ces justifications ponctuelles et parfaitement classiques du point de vue de l'analyse politique, nous plaidons pour une reformulation des défis numériques auxquels les forces armées françaises doivent faire face. Les dangers issus d'Internet et de la communication entre réseaux informatiques sont bien compris et n'ont plus besoin d'être « survendus » à l'opinion et au législateur[11].

II) Les problèmes de la numérisation de l'espace de bataille

Introduisant la notion de « cyberespace » et de « cyberguerre », le LB de 2008 proposait déjà un programme de « Lutte informatique offensive (LIO) », devant permettre à la France de répliquer aux attaques numériques et de provoquer, grâce à une combinaison adéquate avec les forces cinétiques, de démultiplier les effets de la force conventionnelle, et de faire baisser les coûts de sa projection. « La planification et l'exécution d'opérations combinées avec des actions cybernétiques tendent en effet à devenir la norme. Avant même que des cibles physiques ne soient détruites, tout

[7] Thomas Rid, *Cyberwar will not take place*, Londres, Hurst, 2017 (2nd ed.)
[8] Isaac R. Porche III & Clarke P. Colin, *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*, Santa Monica, RAND Corporation, Aroyo Center, 2017.
[9] "Strategic Cyberspace Operations Guide", *United States Army War College*, Carlisle, Pennsylvania, juin 2016.
[10] Terme très souvent employé dans le Livre Blanc de 2013
[11] Emilio Iasiello, "Are Cyber Weapons Effective Military Tools?" in *Military & Strategic Affairs*, vol.7, n° 1, march 2015.

système de défense pourra être en effet désorganisé et partiellement aveuglé au travers de frappes silencieuses et ciblées »[12]. Nous noterons l'abandon, précoce, du préfixe cyber- pour décrire ces opérations, qui participent directement à l'effort militaire et ont pour objectif de minimiser le danger auquel font face les soldats.

Le LB de 2013 insiste quant à lui beaucoup sur la constitution d'une « cybermenace » élargie et discrimine de manière satisfaisante ce qui est du domaine de la délinquance et de la mission de protection de l'État.

> « Relèvent de la sécurité nationale les tentatives de pénétration de réseaux numériques à des fins d'espionnage, qu'elles visent les systèmes d'information de l'État ou ceux des entreprises. Une attaque visant la destruction ou la prise de contrôle à distance de systèmes informatisés commandant le fonctionnement d'infrastructures d'importance vitale, de systèmes de gestion automatisés d'outils industriels potentiellement dangereux, voire de systèmes d'armes ou de capacités militaires stratégiques pourrait ainsi avoir de graves conséquences. Le cyberespace est donc désormais un champ de confrontation à part entière »[13].

La question du commandement des nouvelles capacités y est abordée brièvement et révèle une véritable tension intellectuelle entre, d'un côté, les tenants d'un milieu à part entière et, de l'autre, ceux d'une meilleure intégration des forces armées grâces aux outils numériques et à l'utilisation très rapide des données du renseignement :

> « Le développement de capacités de cyberdéfense militaire fera l'objet d'un effort marqué, en relation étroite avec le domaine du renseignement. La France développera sa posture sur la base d'une organisation de cyberdéfense étroitement intégrée aux forces, disposant de capacités défensives et offensives pour préparer ou accompagner les opérations militaires. *L'organisation opérationnelle des armées intégrera ainsi une chaîne opérationnelle de cyberdéfense, cohérente avec l'organisation et la structure opérationnelles de nos armées, et adaptée aux caractéristiques propres à cet espace de confrontation* »[14]. Le document précise que cette « chaîne opérationnelle » numérique doit être « centralisée à partir du centre de planification et de conduite des opérations de l'état-major des armées, pour garantir une vision globale d'entrée et une mobilisation rapide des moyens nécessaires »[15].

Cette voie, et non celle d'une « cyberarmée », a été effectivement privilégiée pour la création du COMCYBER, opérationnelle depuis le 1er janvier 2017. Celui-ci aura pour mission de coordonner, sous l'autorité directe du Chef d'État-Major des Armées l'ensemble de l'action numérique des armées, de façon transversale à toutes les composantes. Le refus d'en faire une entité séparée et son implantation au cœur même des services centraux de commandement des armées (sur le modèle du CYBERCOM américain, crée en 2010 et intégré au *Joint Commandement)*, montre de manière parfaitement claire que ces composantes informatiques sont au service des toutes les armées et toutes les armes. C'est le même esprit qui a présidé, au sein du nouveau modèle d'armée « Au Contact », à constitution d'un COMSIC centralisé (commandement des systèmes d'information et de communication), créé le 1er juillet 2016 à Cesson-Sévigné, grâce à la fusion des divisions SIC d'appui au commandement et de l'état-major de la Brigade de Transmissions et d'Appui au Commandement (BTAC), auxquels ont été adjoints la Direction Études et Prospective (DEP) et l'École des Transmissions (ETRS), auparavant disséminés sur tout le territoire national.

---

[12] Livre Blanc de la Défense et de la Sécurité Nationale, 2008, p.207. Ce fut le cas lors de l'offensive israélienne sur les installations nucléaires syriennes de Deir-ez-Zor en 2007, qui désactiva à distance les défenses aériennes de cette région pour frapper sans danger le réacteur en construction.
[13] Livre Blanc de la Défense et de la sécurité Nationale de 2013, p.45.
[14] *Ibid.*, p.94. Nous soulignons.
[15] *Ibid.*

III) Commander à l'âge numérique

Comme le souligne le document *Chocs Futurs* publié en avril par le SGDSN, toutes les armées seront affectées par ce mouvement de numérisation. Les microdrones de reconnaissance, les drones armés et à très longue portée, les robots et systèmes autonomes de combat, les capteurs de renseignements seront indispensables pour améliorer les capacités opérationnelles ou en diminuer le coût humain : déminage, repérages en zones hostiles, interventions en terrain contaminé, sécurisation des emprises, évacuation et aide aux blessés[16].

Enfin, la Revue Stratégique sanctuarise cette approche en apportant quelques précisions sur l'esprit devant présider à l'intégration d'officiers et de sous-officiers numériques à tous les échelons de la hiérarchie. Au paragraphe 299, nous pouvons lire que

> « les armées doivent enfin planifier et conduire les opérations dans l'espace numérique jusqu'au niveau tactique, de façon totalement intégrée, à la chaîne de planification et de conduite des opérations cinétiques. *En plus des opérations spécifiques au cyberespace, les opérations dans l'espace numérique élargissent la palette des effets traditionnels à la disposition des autorités politiques* et exploitent la numérisation croissante de nos adversaires, étatiques ou non. Cette aptitude nécessite une ressource humaine renforcée et suffisamment agile, ainsi que le développement permanent de solutions techniques spécifiques »[17].

Durablement engagée vers l'intégration et la synchronisation de ses forces conventionnelles avec les outils numériques, la France a d'ores et déjà opté pour l'intégration cyber-tactique et a abandonné l'idée séductrice mais trompeuse d'une « 4e armée cyber », dérivée de l'application stricte du concept de « continuum sécurité-défense. En cela, la Revue Stratégique préfigure la mise en place à tous les échelons d'officiers, de sous-officiers qui permettront de planifier et d'exécuter les objectifs numériques en totale synchronisation avec ceux, plus généraux, de la mission. La présence à des milliers de kilomètres d'équipes dédiées au "cyber" (opérateurs drone, équipes de piratage), ne permet pas la congruence des deux équipes, et abouti souvent à l'annulation de la mission au moindre accroc au plan de départ, car la communication entre la hiérarchie et l'équipe numérique ne se fait pas de manière optimale. Sans esprit de corps, les équipes situées sur le territoire national se sentent moins solidaires des troupes envoyées en OPEX. L'armée américaine a ainsi mis en place cette année une hiérarchie complète d'*Electronic Warfare Officiers* (EWO) et de managers du spectre électromagnétique, devant être incorporés à tous les niveaux de la chaîne de commandement[18].

Conclusion : Pour une politique de défense numérique

Le rôle des outils de "guerre électronique" dans "le dernier kilomètre tactique" [19] s'avère, à chaque confrontation, un peu plus primordial. Il a d'ores et déjà permis à des groupes comme l'État

[16] *Chocs Futurs*, SGDSN, avril 2017, p.192-196.
[17] *Revue Stratégique*, 2017, p.83.
[18] Voir le "Field Manual 3-12 – Cyberspace and Electronic Warfare Operations", Joint Publications, *United States Department of Defense*, avril 2017, chapitre 3 (Corps to brigade-level electromagnetic cyberspace operations). Il remplace le FM 3-12 (R) de 2013, intitule simplement "Cyberspace Operations" et y ajoute la notion d'Electronic Warfare, utilisé désormais par l'armée française sous la traduction de "Guerre Electronique" (GE), notamment dans le modèle d'armée "Au Contact".

[19] Terme utilisé notamment par Isaac R. Porche III & Clarke P. Colin, *Tactical Cyber*, *op. cit.*, p.26.

Islamique ou le Front Al-Nosrah de mener des opérations *low tech* et *low budget* de plus en en plus sophistiquées et de plus en plus difficiles et couteuses à combattre.

Notre démarche, présentée ici succinctement, cherche avant tout à éviter un écueil dans lequel la Défense Nationale ne doit pas tomber : celui de la séparation trop grande entre opérations numériques et conventionnelles, en pensant de manière trop radicale l'altérité entre le nouveau champ de conflictualité et l'ancien, sur le mode du 4e milieu et de la 4e armée. Ouvert depuis 2008, ce chantier, abordé par la Revue Stratégique, est crucial pour maintenir la capacité de la France, "puissance mondiale moyenne", à agir et à imposer sa volonté sur la scène internationale.

Ne pas faire du cyber un espace propre, et donc ne pas considérer qu'il est le 4e domaine de la guerre, avec sa stratégie propre, n'est pas le déconsidérer ou en minorer le rôle. Bien au contraire, c'est insister sur la transversalité totale du système technique numérique et le placer au centre de toutes les opérations relevant du ministère de la Défense. C'est aussi considérer que sa place est centrale dans la prise de décision et qu'une bonne intégration organisationnelle est gage d'une meilleure agilité tactique et d'une capacité d'improvisation et d'adaptation aux situations imprévues renforcée.