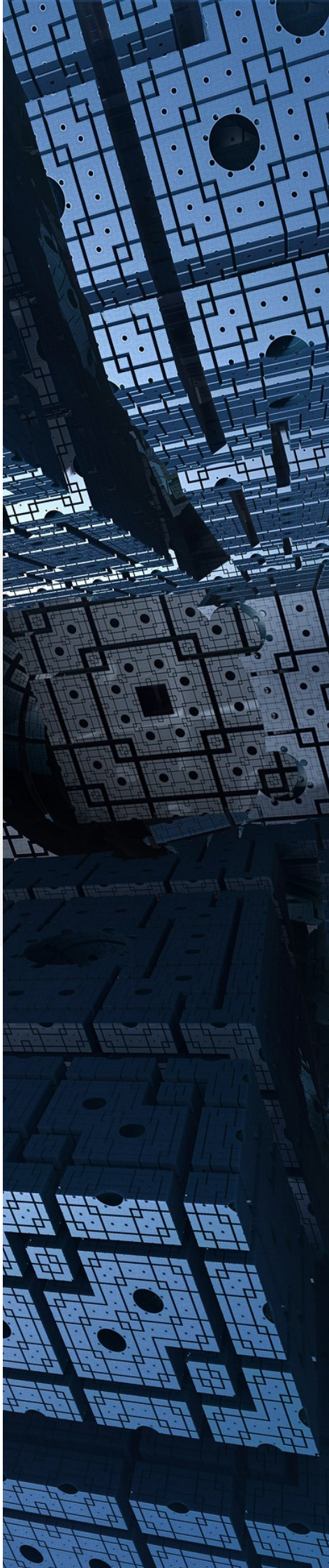
iesd
Institut d'études de stratégie et de défense
Faculté de droit
Université Jean Moulin - Lyon III



MAI 2020

L'intégration numérique des armées

De l'incorporation tactique à la conjonction stratégique

Antony Dabila

NOTE DE **RECHERCHE**

Analyse technico-capacitaire

A propos de l'IESD

L'Institut d'études de stratégie et de défense (IESD) est une structure de recherche universitaire créée en 2018 et spécialisée dans le champ des études stratégiques. Soutenu par l'Université de Lyon (UdL), l'IESD appartient à la **faculté de droit de l'université Jean Moulin – Lyon III**. L'institut, ancré dans la discipline de la science politique et la branche des Relations internationales, accueille une équipe multidisciplinaire de chercheurs lyonnais et extérieurs, (droit, science politique, sciences de gestion, économie, histoire) et fédère autour d'elle un réseau d'experts, de chercheurs, de doctorants et d'étudiants spécialisés dans le champ des études stratégiques.

L'IESD est actuellement partie prenante de la candidature à la **labellisation « Centres nationaux d'excellence défense » de la DGRIS** (ministère des Armées), dans le cadre d'un programme de recherche intitulé « *L'interconnexion des capacités stratégiques hautes (puissance aérienne, espace, nucléaire, défense anti-missiles) : conséquences politiques et opérationnelles des couplages capacitaires de haute intensité dans les espaces homogènes et les Contested Commons* ».

Directeur de l'IESD : **Olivier Zajec**
Directeur de collection : **Antony Dabila**

Contact : iesd.contact@gmail.com

IESD – Faculté de droit
Université Jean Moulin – Lyon III
1C avenue des Frères Lumière – CS 78242
69372 LYON CEDEX 08

iesd
Institut d'études de stratégie et de défense
Faculté de droit
Université Jean Moulin - Lyon III

NOTE DE RECHERCHE

Analyse technico-capacitaire

Antony Dabila, « *L'intégration numérique des armées, de l'incorporation tactique à la conjonction stratégique* », *Notes de Recherche de l'IESD*, coll. « Analyse technico-capacitaire », n°6, mai 2020.

Résumé

La mise en place d'outils numériques dans les armées a entraîné des bouleversements organisationnels et humains qui ne peuvent être appréhendés d'un simple point de vue technique ou technologique. À l'hypothèse d'un milieu « cyber » distinct des autres fonctions des armées, nous proposons de substituer une analyse humaine et sociologique centrée sur le processus de « numérisation des forces ». Ce décentrement débouche sur plusieurs concepts qui permettent de compléter et d'enrichir l'analyse des processus de prise de décision stratégique. De ce point de vue, la création d'unités dédiées à la lutte informatique n'est sans doute que l'une des étapes nécessaires à une « intégration numérique des armées », laquelle nécessitera *in fine* une transformation et une adaptation de l'ensemble des forces au nouveau système technique de commandement et de coordination numérisé. Il semble dès lors nécessaire de distinguer « l'incorporation numérique tactique » de la « conjonction numérique stratégique », afin de remettre en perspective les dynamiques futures du processus de transition numérique des armées.

Abstract

The implementation of digital tools in the armed forces has led to upheavals at both an organizational and human level, which cannot be understood from a simple technical or technological point of view. For this reason, this paper focuses on conducting a human and sociological analysis centered on the process of "digitization of armies" rather than analyzing cyber separate from the rest of the armed forces. This change of perspective makes it possible to identify several concepts that complement and enrich the analysis of strategic decision-making processes. From this point of view, the creation of tactical-level units dedicated to computerized warfare is only one necessary step in the "digital integration of armies", requiring the transformation and adaptation of all forces to the new digitized technical command and coordination system. It is; therefore, necessary to distinguish between "tactical digital incorporation" and "strategic digital conjunction" in order to complete an assessment of the armed forces' digital transition processes.

À propos de l'auteur

Antony Dabila est post-doctorant à l'Institut d'Études de Stratégie et de Défense. Ses recherches portent sur les transformations du milieu humain constitué par les combattants et la manière dont la pensée stratégique s'adapte à ses transformations. Il enseigne la stratégie et les politiques de défense et de sécurité à l'université Lyon-III-Jean Moulin, Sciences Po Lyon et l'Institut Mines Télécom.

Table des matières

Numérisation et réticulation : nouvelles problématiques de commandement

Depuis la fin de la Guerre froide, l'un des faits stratégiques majeurs est sans conteste l'utilisation désormais massive de moyens numériques de communication, d'observation et d'analyse par l'ensemble des forces armées des principales puissances militaires, qu'elles soient à vocation mondiale ou régionale. Ce phénomène, pour bien des analystes, renvoie à la création d'un nouveau domaine de la guerre, le « cyber ». Cette étiquette englobante pose un certain nombre de problèmes lorsqu'il s'agit de comprendre et d'anticiper les conséquences opérationnelles de cette transformation. Dans cette note, nous poserons comme hypothèse qu'il serait à bien des égards préférable de définir ce phénomène dans le cadre d'une tension complémentaire entre d'une part une *numérisation* des armées et d'autre part une dynamique *d'intégration numérique* des forces.

L'objectif des réflexions exploratoires qui suivent est ainsi de souligner les conclusions différentes auxquelles l'analyste du fait militaire est conduit, selon qu'il considère le processus d'introduction extensive de l'informatique dans le combat soit comme la création d'un « milieu » supplémentaire, soit comme une numérisation globale de l'outil militaire, de manière à éclairer les enjeux de ce double éclairage. Nous rappellerons ici la doctrine qui préside à l'implantation des moyens numériques dans les armées françaises, en comparant celle-ci aux évolutions des forces américaines en la matière, ces dernières tendant en effet à définir les tendances, à la fois techniques et conceptuelles, en matière d'innovation de défense.

Le terme « cyber », pris à la fois comme préfixe et comme substantif, s'est imposé dans le discours stratégique afin de désigner l'ensemble technique informatique surajouté aux moyens de défense traditionnels. Ce mot rassemble pourtant des domaines et des savoir-faire très différents, qui traitent de menaces auparavant confiées à des agences de l'Etat spécialisées. Prenons pour exemple la dernière version, datée de juillet 2019, du document doctrinal français intitulé *Stratégie du Renseignement*, publié par la Coordination Nationale du Renseignement et de la Lutte contre le Terrorisme. Ce service, dépendant directement de la Présidence de la République, liste dans ce document les menaces « en matière cyber » comme suit : « la menace, qu'elle soit étatique, provenant d'entreprises privées ou d'organisations criminelles, a fortement évolué. Elle est de plusieurs natures : *vol de données, sabotage au préjudice des entreprises comme des administrations, pénétration aux fins d'espionnage, chantage en vue d'obtenir une rançon*… Il convient de souligner que certaines de ces opérations de prédation relèvent désormais d'une nouvelle forme de cybercriminalité organisée »[1]. Ce document ajoute que « *[…] par le biais d'Internet et des réseaux sociaux, l'espace cyber est un vecteur de diffusion des messages haineux et de manipulation de l'information qui mérite un suivi du Renseignement, notamment en termes de lutte contre la cybercriminalité, pour identifier les messages ou les campagnes les amplifiant, en attribuer l'origine et faciliter leur entrave administrative et judiciaire* »[2].

Ainsi, ce document fait-il un usage extensif du préfixe « cyber- », qu'il accole à une nuée de phénomènes disparates pour leur donner corps. Ces moyens d'action disparates, menés par des acteurs hétérogènes n'ayant pas forcément de visées politiques, sont rassemblés sous une même catégorie, nécessitant une action coordonnée et des services communs. Or, si elles n'utilisaient pas comme vecteur commun le réseau informatique mondial nommé Internet, ces mêmes actions auraient relevé bien entendu des services de renseignement, aussi ceux de la police que ceux des forces armées.

[1] « Stratégie Nationale du Renseignement », Coordination Nationale du Renseignement et de la Lutte contre le Terrorisme, Paris, juillet 2019, p.6. Nous soulignons.

[2] *Ibid.*

Leur rassemblement dans une même catégorie devant être traitée de manière uniforme par un ou des services étatiques dédiés n'a donc rien d'évident. Aussi semble-t-il prudent de s'interroger sur la pertinence de cette catégorisation pour aborder le phénomène de la numérisation des forces. Nous pouvons ainsi, dès l'abord, poser la question qui nous occupera dans cette note : le phénomène de numérisation partielle des affrontements militaires se limite-t-il à la création d'unités dédiées et fonctionnellement spécialisée, ou bien nécessite-t-il au contraire la mise en place d'éléments numérisés à l'intérieur de chaque unité, pour faire face de manière proportionnée et contextualisée aux avatars extrêmement divers du défi générique que constituent les « cyber-menaces » ? En d'autres termes, c'est bien la question du mode de *réticulation numérique* le plus pertinent qui se pose pour les forces armées. De la réponse à cette question dépend la stratégie de transformation numérique des forces armées qui pourrait être choisie par le gouvernement afin de fondre les différentes agences dans un nouveau format, destiné à tirer le meilleur parti des possibilités des communications informatiques à distance.

Né dans le domaine de la science-fiction en 1984, sous la plume de l'écrivain William Gibson[3], le terme « cyber » s'est rapidement propagé après l'ouverture complète du réseau informatique « *world wide web* » au public, le 1er janvier 1990. Il tend à désigner le réseau créé par l'interconnexion des données stockées et produites par les ordinateurs, répartis sur l'ensemble de la planète. Il peut donc être considéré comme un « espace » dans lequel il est possible de se déplacer pour « saisir » et exploiter des données, quel que soit leur lieu de création ou de stockage. Peu à peu, le terme s'impose dans les doctrines stratégiques, en particulier après l'influent article de John Arquilla et David Ronfeld, *Cyberwar is Coming !*, publié par la RAND Corporation en 1993[4].

Ce que nous indique l'émergence de ce nouveau vocabulaire est qu'à ce « milieu », dernier-né des espaces de déploiement des opérations militaires, aurait dû forcément correspondre un genre inédit de guerre et de stratégie. Une telle logique serait d'une certaine façon la transposition de la pensée de l'amiral Alfred T. Mahan, voulant qu'à un « espace » particulier de la confrontation guerrière corresponde une espèce particulière de stratégie d'action et de dissuasion, possédant ses propres règles. Cet élargissement de la stratégie lié à l'apparition d'un nouveau milieu a été appliqué à raison et de manière convaincante à l'espace aérien lors de la Première Guerre mondiale.

Depuis la Seconde Guerre mondiale, la même logique s'est progressivement imposée dans le domaine spatial, avec la première course à l'espace des années 1950-1960 et, plus récemment, avec l'annonce récente de la création d'une *US Space Force*[5] et d'un Commandement des Forces Spatiales pour la France. L'espace extra-atmosphérique constitue ainsi à présent le quatrième milieu spécifique de l'affrontement guerrier, quoique la pertinence d'une armée dédiée (ou « composante ») soit encore fortement contestée[6]. Notons cependant que le domaine sous-marin, bien que doté de caractéristiques physiques très différentes, est vu de manière à peu près consensuelle comme une extension du domaine maritime[7].

Dans ces conditions, il est possible de se demander s'il est légitime de parler d'un « milieu numérique » entièrement composé d'ondes électromagnétiques et de données informatiques. Corolairement, ceci nous conduit à une autre question : ce « milieu » possède-t-il sa stratégie propre ? Le travail conceptuel derrière cette ques-

[3] Gibson, William, *The Neuromancer*, New York, Ace Books, 1984.
[4] Arquilla, John & David Ronfeldt, *Cyberwar is Coming!*, Santa Monica, RAND Corporation, RP-223, 1993.
[5] Cf "Us Space Force Facts Sheet", 19 décembre 2019, Washington, Departement of Defense, https://www.spaceforce.mil/About-Us/Fact-Sheet.
[6] Cf. McCain, John S., "National Defense Authorization Act (NDAA) for Fiscal Year 2019", Public Law n° 115-232, signée par D. Trump en août 2018.
[7] Coutau-Bégarie, Hervé, *Traité de Stratégie*, Paris, Economica, 2011 (7e édition), p.725-6.

tion n'est pas anodin. La manière d'y répondre définira une certaine vision de la « chose » numérique et influencera par conséquent de manière très concrète la prise de décision dans ce domaine, dans la mesure où le schéma choisi pour l'architecture numérique de défense est le préalable à la transformation numérique des forces.

En effet, au-delà de la question d'une « quatrième » armée (ou cinquième si les forces spatiales se généralisent dans la continuité de la récente décision américaine), le point crucial est de savoir comment intégrer des unités numériques aux forces combattantes et, en fonction de l'orientation retenue, de décider à quel niveau du dispositif militaire les placer.

Corolairement, le problème du meilleur modèle de commandement se pose pour alléger au maximum la boucle d'ordres et de commandements qui relie les niveaux tactique, opératif et stratégique de l'action militaire. Pour répondre à ces questions, nous examinerons les mesures en cours d'application dans les armées françaises et américaines en termes de numérisation des forces combattantes[8]. Cela nous permettra d'observer si cette transition informatique du système technique militaire est réellement pensée sur le patron d'un milieu indépendant ou bien sur celui d'une numérisation des outils existants et de l'implantation d'un nouvel « ensemble technique »[9] de communication, transversale à tous les autres milieux.

Les communications informatiques à distance : nouvelle source d'insécurité transpolitique

La palette des agents de la nouvelle « insécurité numérique » n'a cessé de s'élargir depuis vingt ans : y appartiennent les États *via* leurs forces de sécurité et de renseignement, les groupes dissidents et insurrectionnels, les organisations criminelles, ainsi que les individus malveillants et en recherche de défis quasi-sportifs de pénétration et de dégradation des systèmes informatiques[10]. Si l'on voulait le résumer de manière abrupte, on pourrait dire que l'apparition de l'informatique, puis d'Internet, a renforcé les acteurs privés sur la scène transpolitique[11], tout en amoindrissant encore un peu plus la place occupée par les États sur celle-ci.

C'est l'ensemble de ces comportements agressifs au moyen des réseaux informatiques, et des opérations visant à s'en défendre, qui ont été rassemblé sous le concept de « cyberguerre ». Le terme est cependant contesté par d'éminents spécialistes de ce domaine. Eugène Kaspersky, fondateur de l'entreprise de cybersécurité du même nom, conteste l'idée même que le conflit numérique prolongerait symétriquement celui de la réalité : « *Les attaques que nous connaissons aujourd'hui ne donnent aucun indice sur celui qui les a commises et s'ils vous frapperont à nouveau. Ce n'est pas de la cyberguerre mais plutôt du cyberterrorisme* »[12]. Le spécialiste russe poursuit la réfutation du terme et du concept même en considérant le statut des « armes » avec lesquelles cette guerre serait menée. *« Les cyberarmes peuvent avoir des effets boomerang. Un missile, on ne peut pas l'attraper, le démonter, le réassembler et le renvoyer ; une cyberattaque, si. Vous pouvez la copier, la modifier et la renvoyer. Certes, l'opération n'est pas facile,*

[8] Rapport parlementaire Becht-Gassilloud n° 996 portant sur « Les enjeux de la numérisation des armées », mai 2018.
[9] Selon l'acception de Gilbert Simondon, *Du Mode d'existence des objets techniques*, Paris, Aubier-Montaigne, 1958.
[10] "Field Manual 3-12 (R) – Cyberspace Operations", Joint Publications, *United States Department of Defense*, février 2013, p.19-20.
[11] Si l'espace politique interne est défini par la présence d'outil de pacification tendancielle, l'espace extérieur à l'unité politique peut être défini comme un espace de conflit potentiel. C'est cet espace mettant aux prises les unités politiques (ou « polities ») que nous que nous qualifions de « transpolitie » et dont l'adjectif dérivé est « transpolitique ». Cf Jean Baechler, *Nature et Histoire*, Paris, PUF, 2000, pp.80-93
[12] "Latest Viruses Could Mean 'End Of World As We Know It,' Says Man Who Discovered Flame", *Times of Israel*, 6 juin 2012.

mais c'est possible. Et c'est une opération beaucoup plus aisée que la construction d'un missile, bien sûr »[13]. Une fois utilisé, le moyen même de l'agression peut porter atteinte à la sûreté informatique de son auteur. Nous sommes là dans le domaine de la sécurité plutôt que dans celui de la Défense, à moins d'identifier l'un à l'autre. Dans ce cas, la spécificité politique de la guerre serait alors perdue.

La propriété principale de ces attaques réside donc dans le fait de ne pouvoir être attribuées que de manière fastidieuse et incertaine, bien après que l'action soit déroulée[14]. Certains groupes peuvent ainsi dissimuler leurs véritables objectifs derrière des revendications factices et invérifiables. Ainsi, les agissements de groupes « pirates » peuvent être détournés ou soutenus en sous-main pour réaliser du vol de propriété intellectuelle ou déstabiliser un concurrent. Dans un autre registre, la Russie a pu profiter d'attaques « spontanées » de groupes de *hackers* dans ses actions internationales contre l'Estonie en 2007, la Géorgie en 2008 et l'Ukraine en 2014. Toutes ont contribué à atteindre l'objectif politique de ces opérations : punir un manque de respect des soldats soviétiques de la Seconde Guerre mondiale de la part du gouvernement estonien, désorganiser la riposte armée des gouvernements de Tbilissi et de Kiev.

Conséquence de cette impossibilité – ou de cette très grande difficulté – d'attribuer les attaques, la nature de la confrontation n'est pas comparable à une guerre, avec des lignes de contact et une période bien établies, ni même à une guérilla cherchant à saper l'ordre politique et à en montrer les faiblesses. Il s'agit d'un conflit diffus et permanent, dans lequel aucun état de paix ne succédera à un état de guerre. Les actions à visée politique ne sont que des épisodes de plus grande intensité, au milieu de tentatives constantes pour contourner les défenses disposées autour des données et des infrastructures constituant le réseau. Selon Eugène Kaspersky, cité précédemment, il s'agirait finalement là d'une sorte d'hygiénisme numérique plutôt que d'une politique de sécurité ciblée sur des groupes précis : « *La sécurité traditionnelle n'est pas en mesure de résoudre ce problème. Je pense qu'on doit passer de la cybersécurité à ce que j'appelle de la cyber-immunité. On doit concevoir une nouvelle architecture informatique afin qu'il soit beaucoup plus compliqué de pirater, voire impossible* »[15].

Cette vision, qui ne limite pas la défense numérique à sa dimension sécuritaire, invite à bâtir l'architecture de circulation et de sécurisation des données en s'inspirant d'autres champs de comparaison, notamment celui de la médecine : « *Aujourd'hui, conclut Kaspersky, on ajoute des couches de protection à une architecture déjà existante. Est-ce que ce ne serait pas plus simple de mettre des solutions sécurisées dès la conception ? […] Autour de nous, on sait que gravitent plein de microbes, et ils ne nous atteignent pas, parce que nous sommes plus ou moins immunisés. De temps en temps, on a un rhume. Pour l'instant, les systèmes connectés ne sont pas immunisés, parce qu'ils ne sont pas conçus pour. Pour qu'ils le soient, il faut repenser leur conception. Le travail va être long. On propose déjà une solution de cyber-immunité pour l'Internet des Objets* »[16].

Cependant, les agents de la nouvelle « insécurité numérique » constituent bien une menace, et sont d'ores et déjà des acteurs à part entière des batailles « physiques » ou « cinétiques » se déroulant entre forces armées. Cette menace diffuse et très diverse ne relevait pas (ou peu) de la compétence des forces armées avant leur « numérisation », mais plutôt de celle d'agences de renseignement civiles. C'est seulement à mesure que ces menaces se sont immiscées sur le champ de bataille, en interagissant avec certains dispositifs

[13] Kaspersky, Eugène, « Cyberguerre : « il n'y a aucune preuve » selon Eugène Kaspersky » in *Usbek et Rica,* 29 juin 2019, Consulté le 10 juillet 2019, https://usbeketrica.com/article/cyberguerre-il-n-y-a-aucune-preuve?fbclid=IwAR1PZybPmU6qyr520VafxmbC3SSXL0qxPOElOhEP-uh9UeUGooIKtIfqohk

[14] Kempf, Olivier, *Alliances et mésalliances dans le cyberespace*, Paris, Economica, 2014.

[15] Kaspersky, Eugène, « Cyberguerre : « il n'y a aucune preuve » selon Eugène Kaspersky », *op. cit.*

[16] *Ibid.*

physiques ou bien en dérobant des informations utiles à la conduite des combats que leur véritable portée a peu à peu été saisie. Cependant, si les défis auxquels les armées devront faire face deviennent plus tangibles, la place du combat numérique dans la conduite de la guerre n'est pas pleinement précisée, même à un horizon de cinq ou dix ans.

Cette imprévisibilité de l'évolution est due à deux caractéristiques propres à l'affrontement numérique : l'utilisation effective constante des techniques permettant de s'introduire et d'endommager les réseaux adverses, ainsi que la rapidité intrinsèque de l'évolution de ces techniques. Contrairement à l'arme atomique ou à la puissance aérienne, où l'unité de temps est plutôt la décennie que l'année, le cycle d'acquisition des nouvelles technologies a tendance à se mesurer en mois, comme le souligne le général Nakasone, commandant du US CyberCom depuis 2018 : « *Contrairement au domaine nucléaire, où notre avantage stratégique ou notre puissance vient de la possession d'une capacité ou d'un système d'armes, dans le cyberespace, c'est l'utilisation de cyber-capacités qui est stratégiquement conséquente. La menace d'utiliser quelque chose dans le cyberespace n'est pas aussi puissante qu'en réalité parce que c'est ce que nos adversaires nous font. Ils s'introduisent activement dans nos réseaux de communications, tentent de voler des données et cherchent à avoir un impact sur nos systèmes d'armes. L'avantage est donc gagné par ceux qui se maintiennent en position d'agir continuellement* ». Il est donc impossible de connaître l'état du champ de bataille numérique à un horizon de cinq ans, car cela supposerait de connaître une dizaine de générations de malware. « *Lorsque nous achetons une capacité ou un outil pour le cyberespace, poursuit le général Nakasone, nous obtenons rarement une utilisation prolongée que nous pouvons mesurer en années. Nos capacités durent rarement 6 mois, encore moins 6 ans* »[17].

Depuis l'invasion de la Crimée et la formation de l'Etat Islamique, les six dernières années ont permis de préciser la place que tend à occuper l'utilisation des technologies informatiques de nouvelle génération dans le domaine militaire. Auparavant difficile à prévoir, l'utilisation concrète des nouvelles technologies *à l'intérieur de l'espace de bataille* s'est en effet grandement précisée depuis les épisodes belliqueux liés aux printemps arabes et à la guerre du Donbass. Nous avons ainsi 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[18]. En particulier, la guerre en Syrie et en Irak a permis d'observer les conséquences opérationnelles d'une généralisation du recours aux moyens numériques, dans un grand nombre de domaines (commandement, communication, reconnaissance, renseignement, propagande, recrutement, revendication, etc.).

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[19]. En conséquence, cette volonté a fait des affrontements de la guerre civile syrienne un véritable laboratoire, où il est possible d'entrevoir le rôle que sont appelées à jouer les nouvelles

[17] Interview du general Nakasone dans *Joint Forces Quarterly*, n° 92, 1er trimester 2019, pp.4-9. "*Unlike the nuclear realm, where our strategic advantage or power comes from possessing a capability or weapons system, in cyberspace it's the use of cyber capabilities that is strategically consequential. The threat of using something in cyberspace is not as powerful as actually using it because that's what our adversaries are doing to us. They are actively in our network communications, attempting to steal data and impact our weapons systems. So advantage is gained by those who maintain a continual state of action. [...] When we buy a capability or tool for cyberspace we rarely get a prolonged use we can measure in years. Our capabilities rarely last 6 months, let alone 6 years*".

[18] "Strategic Cyberspace Operations Guide", US Army War College, Carlisle, Pennsylvania, juin 2016, p.9.

[19] Brynjar, Lia, *Architect of global Jihad*, London & New York, Hurst &Columbia University Press, 2008.

technologies numériques dans la poursuite du combat et la conduite de la guerre[20]. Ainsi, la manière dont sont en train de s'implanter les technologies numériques, dans toutes les dimensions de l'affrontement, montre le dévoilement d'une logique sous-jacente qui est celle d'une numérisation des instruments de violence et de combat, en vue d'obtenir des effets politiques sur la scène transpolitique.

Dans le domaine de la sécurité civile, l'épisode dit « Wannacry », qui a bloqué une partie des hôpitaux londoniens en mai 2017, a fait prendre conscience de l'ampleur que pourrait revêtir une attaque coordonnée, et ses conséquences potentielles sur le quotidien et l'économie des pays européens, y compris les plus puissants militairement. Les récentes attaques iraniennes sur le réseau de production d'eau israélien et les représailles de l'État hébreu sur le port de Bandar Abbas[21] illustrent encore un peu plus l'ampleur que pourrait revêtir le sabotage numérique. Que se serait-il passé si ces blocages s'étaient produits pendant un épisode de tension, comme la crise du COVID-19, ou bien pendant un affrontement ? Le blocage du terminal de Shahid Rajaee montre en tout état de cause que les chaînes d'approvisionnement pourraient être grandement impactées par un assaut numérique.

En définitive, il semble que l'on assiste à une numérisation accélérée des armes permettant de conduire la guerre, voire d'une autonomisation de certains dispositifs violents. Cette évolution, annoncée depuis longtemps, surprend néanmoins par la soudaineté de sa diffusion. Porté par la démocratisation accélérée des technologies, par les bénéfices évidents qu'en retirent les « techno-guérillas »[22], mais aussi par la course à la maîtrise technologique entre grandes puissances (en particulier dans le portfolio que constituent les capacités stratégiques hautes), le mouvement de numérisation concerne tous les domaines et toutes les composantes. Tout ceci suggère que l'on ne voit finalement pas se constituer à proprement parler un espace de guerre numérique séparé, mais plutôt la mise en place d'instruments de production et de communication d'informations formant un nouvel espace de communication numérisé.

Suivant un terme proposé par Jean Baechler, il nous apparait utile d'envisager cet espace comme un type nouveau d'« *agorie* », c'est-à-dire comme un espace où la communication et l'échange d'informations sont permis et conditionnés par leurs déterminants sociaux et techniques[23]. Cette « agorie » prend place au sein de la nouvelle « agorie numérique mondiale » créée par la communication informatique à distance, dont la manifestation la plus connue est Internet. Partant, nous proposons de parler de l'espace social créé par l'irruption des outils de ce genre dans l'affrontement guerrier comme d'une nouvelle « **agorie numérique militaire** », dont l'existence, et les possibilités qu'elles renferment, modifie nécessairement la nature de l'affrontement militaire. En effet, selon la seconde « action réciproque » de Clausewitz, la guerre est définie par l'impossibilité même de contrôler les moyens par lesquels s'effectue le combat, car l'adversaire me dicte sa loi comme je lui dicte la mienne[24]. Si bien que l'utilisation de l'« agorie numérique militaire » est condamnée à être utilisée si elle permet à l'un des camps d'obtenir un quelconque avantage et de rééquilibrer l'affrontement en sa faveur. Les moyens techniques numériques dans l'affrontement (et non pas seulement autour du champ de bataille) doivent donc être pensés et anticipés, afin de ne pas subir de surprise stratégique[25].

---

[20] Andress, Jason & Winterfeld, Steve, *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners*, Amsterdam, Syngress, 2011, p.5.

[21] "Israel Behind Cyberattack That Caused 'Total Disarray' At Iran Port" in *Times of Israel*, 19 mai 2020, https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/?fbclid=IwAR0QCZ2XzYBOCzNw8yWUqdHfsf71U7_cl9rHS3HsmjMI4uvmgUhBAwC19E4

[22] Henrotin, Joseph, *Techno-guérilla et guerre hybride, le pire des deux mondes*, Paris, Nuvis, 2014.

[23] Baechler, Jean, *Nature et Histoire*, Paris, PUF, 2000, pp.148-160.

[24] Cf Clausewitz, *De la Guerre*, Paris, Editions de Minuit, 1955, Livre I, Chapitre 1, p.52-54.

[25] Comme cela a été le cas pour les précédentes révolutions Steele et Stein dans leur article sur le poids de l'évolution des communications sur la structure de la scène internationale, Steel, Cherie & Stein, Arthur, "Communications Revolutions

La nouvelle agorie numérique militaire : intégration, incorporation et conjonction

L'hypothèse soutenue ici quant à la nature de la « cyberguerre » trouve donc ses contours : le trop grand usage des mots composés à partir du préfixe cyber- (cyberguerre, cyberespace, cybersécurité, cybermenace, etc.) a conduit à une dilatation regrettable du concept[26]. Cette inflation est dommageable, car elle empêche les armées de se concentrer sur leur mission première, qui est, sous l'autorité de la puissance politique, d'employer la force ou la menace de la force pour protéger le territoire et le peuple français des ravages de la violence armée. Or, comme l'affirme Thomas Rid, dans son ouvrage *La Cyber-Guerre n'aura pas lieu*, l'idée de cyber-espace comme « cinquième domaine de la guerre » est un terme métaphorique, principalement porté par l'US Air Force à partir de 2005[27]. Par conséquent, désigner l'ensemble des activités numériques hostiles ou malveillantes comme relevant d'une « cyber-guerre » empêche de voir un fait majeur : l'utilisation d'internet pour l'espionnage et le sabotage a plutôt restreint le domaine de la guerre qu'il ne l'a étendu. En effet, selon Rid, les attaques numériques « *[…] permettent d'atteindre un but qui aurait auparavant demandé l'utilisation d'une certaine quantité de violence politique* »[28]. Il y a donc moins eu extension que substitution. Le choix d'un concept insuffisamment précis a engendré une compréhension confuse de la réalité de la lutte informatique. Ceci s'est révélé dommageable dans la mise en place de politiques publiques visant à doter l'État de corps bureaucratiques destinés à prendre en charge sa numérisation et celle de sa défense.

En raison de cette inadéquation des termes dérivés de « cyber- », peut-être serait-il préférable de désigner le phénomène de transformation numérique du combat au moyen du simple concept de « numérisation des armées ». Ce processus de numérisation comprend plusieurs facettes, qu'il est nécessaire de distinguer.

- D'une part, la mise en place d'unités dédiées uniquement à la lutte informatique et à la protection des infrastructures, des serveurs et des données. Bien que l'on réduise souvent la « cyber-guerre » à ces créations, celles-ci ne représentent que la première étape, nécessaire, à la transition numérique des armées.
- Il faut, en effet, d'autre part et dans un second temps, penser un phénomène qui, à notre sens, se révèle encore plus crucial en termes d'usage de la violence politique. Il s'agit de la mise en place d'un réseau de communication et de transmission des données nécessaires au combat *au sein même* des unités combattantes. Il serait possible de nommer ce phénomène *l'intégration numérique*[29].

Une division classique de la pensée militaire distingue entre les niveaux tactique et stratégique, c'est-à-dire entre utilisation concrète de la force et mise à disposition des ressources nécessaires à l'utilisation de cette force[30]. Cette dichotomie reste pertinente pour penser l'intégration numérique des armées, bien qu'elle charrie avec elle une inévitable confusion concernant la ligne de démarcation précise entre les deux niveaux. Comme l'a démontré

and International Relations", in Juliann Emmons Allison (dir.), Technology Development and Democracy: International conflict and Cooperation in the Information Age, Albany State University of New York Press, 2002, pp.32-35.

[26] Pour une illustration de l'utilisation intensive du préfixe « cyber », cf *infra* le chapitre « Le défi organisationnel et humain de la numérisation », p.19, qui prend l'exemple de la Défense française.

[27] Rid, Thomas, *Cyberwar will not take place*, Londres, Hurst, 2017 (2nd ed.), p.165.

[28] *Ibid.*, p.167.

[29] Voir notre contribution plus spécialement centrée sur ce terme dans notre article « Les évolutions du paradigme cyber : de la 4e armée à l'intégration cybertactique », in *Revue Défense* Nationale, n° 806, janvier 2018.

[30] Cf Dabila, Antony, « L'Engagement militaire : essai de sociologie comparée », thèse soutenue à l'Université Paris-Sorbonne le 5 novembre 2013, chapitre « Disposer et Mettre à Disposition », p.89. https://www.theses.fr/2013PA040132.pdf

Clausewitz, toute action tactique peut en effet posséder une dimension stratégique, et *vice versa*[31].

Conformément à cette division, que l'on peut considérer comme première dans l'activité sociale que constitue la guerre, il s'avère sans doute nécessaire de distinguer plus qu'on ne le fait entre la numérisation du niveau tactique et celle du niveau stratégique. La première insiste sur la transformation du combat lui-même et sur la participation des outils numériques aux actions de force, tandis que la seconde met l'accent sur le caractère global de la mutation, qui concerne l'ensemble des outils de puissance des armées, mais aussi de leurs capacités de renseignement, de commandement et de coordination.

Afin de traduire ces deux phénomènes en des concepts distincts, qu'il est impératif de ne pas confondre, nous proposons de leur attribuer les noms de *numérisation des dispositifs tactiques (de combat)* et de *numérisation des outils stratégiques (de commandement)*.

En raison de l'impossibilité de séparer parfaitement les deux niveaux, nous posons cette distinction tout en sachant que la plupart des actions concrètes passeront fréquemment les barrières entre ces deux processus, naviguant de fait dans une sorte de « glacis numérique » de niveau opératif, qui permettra aux niveaux tactique et stratégique de communiquer. Cette dichotomie tactique-stratégique est davantage un outil permettant de mieux situer et donc interpréter des situations concrètes, plutôt qu'une séparation rigide de deux entités disjointes, que ce soit en planification ou en conduite. Il résulte de cela qu'un ensemble d'opérations numériques appartient par la force des choses aux deux niveaux[32].

Mais ceci ne doit pas masquer ce que ces concepts nous permettent de mettre en relief : la capacité accrue pour les armées de faire converger leurs forces sur des points choisis du dispositif adverse et d'y concentrer la puissance de frappe disponible, grâce aux possibilités inédites offertes par les communications informatiques à distance. Celles-ci autorisent les divers éléments constituant

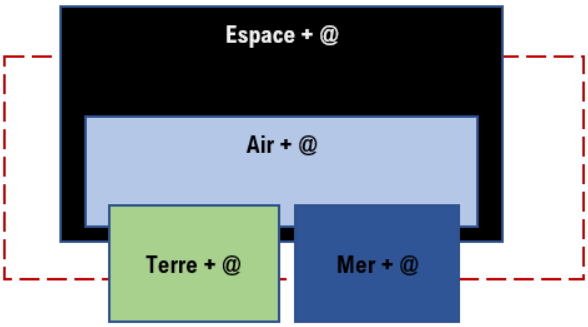


Figure 1 : Les externalités négatives du numérique

une force armée à être de plus en plus *intégrés* et ainsi à produire des effets démultipliés, avec moins de moyens, tout en frappant les points les plus exposés du dispositif de l'ennemi à un instant *t*[33].

Nous opterons finalement pour le terme **d'*intégration numérique des armées*,** tout en séparant, comme le suggère le schéma ci-dessous :

- l'***incorporation numérique tactique*** (Armée x + @) et
- la ***conjonction numérique stratégique*** *(représentée par l'« anneau numérique » en rouge)*.

[31] Clausewitz, *De la Guerre*, Paris, Editions de Minuit, 1955, livre V, chapitre 2, intitulé « Armée, Théâtre de Guerre et Campagne », p. 307.

[32] Sur la notion de « glacis numérique », voir Boyer, Bertrand, *Cybertactique, conduire la guerre numérique*, Paris, Nuvis, 2014.

[33] Voir par exemple la nouvelle doctrine de la « guerre mosaïque », portée par la DARPA et mise au point par David Deptula. Cf « Restoring Americas's Military Competitivness: Mosaic Warfare », par David Deptula et Heather Penney, avec Lawrence Stutzriem et Mark Gunzinger, Arlington (Virginie), The Mitchell Institute for Aerospace Studies, septembre 2019.

Si elle débouche sur des bénéfices certains, la numérisation des armées, qui repose sur une intégration numérique interarmées réussie, fait aussi apparaître de nouvelles faiblesses, qui pourraient entièrement les paralyser. Ces bénéfices sont en effet particulièrement importants dans le domaine du commandement. Or, si cette fonction névralgique est attaquée numériquement, elle risque de paralyser l'ensemble du dispositif interarmées intégré. Les opportunités du numérique portent ainsi en elles leur antithèse, car tout en augmentant les performances des systèmes de commandement et la virtuosité potentielle des « chefs d'orchestre » opérationnels, elles ouvrent aussi des portes dérobées permettant d'atteindre en leur cœur même les dispositifs militaires qui ont tout misé sur cette même intégration numérique.

Grâce à ce double concept, nous cherchons à mieux décrire le processus de transformation selon lequel les nouveaux dispositifs de communication et d'analyse numériques aux fonctions de combat[34], aboutissant à l'établissement d'un *système de communication et de coordination*[35], se reposant pour l'essentiel sur les communications informatiques à distance. Ce système, ayant pour but le raccourcissement des délais de production et de propagation de l'information, a pour caractéristique de numériser l'ensemble de la transmission des ordres au sein des armées et d'automatiser au maximum l'élaboration et la circulation des données sur l'adversaire et sur soi-même.

Ce faisant, un rapprochement des niveaux tactiques et stratégiques s'effectue peu à peu, jusqu'à

Centre de Commandement et de Controle de l'Armée de l'Air Suisse, bon exemple de conjonction stratégique numérique.
Image : Keystone

[34] Porche, Isaac R. III & Colin, Clarke P., *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*, Santa Monica, RAND Corporation, Aroyo Center, 2017.

[35] Nous préférons ce terme à celui de « commande et contrôle », moins explicite, surtout transcris tel quel en français.

remettre en question la manière dont est perçue leur ligne de démarcation. Bien entendu, l'immixtion du niveau stratégique dans le niveau tactique est bien plus forte que l'inverse. C'est la menace dite du « micro-management stratégique », qui constitue, aujourd'hui, une réalité au sein des centres de *Command & Control*[36]. Cet état de fait doit être anticipé lors de la conception des prochains *systèmes de communication et de coordination numériques*, afin de décentraliser au mieux l'exécution des opérations, tout en maintenant la capacité de centraliser l'information pour le commandement.

Cette manière d'appréhender la numérisation de l'outil militaire s'oppose à la volonté de donner à la « cybermenace »[37] un caractère global. Si l'on considère que la tâche des armées est d'assurer la sécurité des citoyens et de l'État dans l'ensemble du spectre des échanges informatiques au niveau mondial, la conséquence inévitable sera de dilater le champ d'action des forces armées et de leur faire manquer le but principal qui leur est imposé par la mutation technologique mondiale : numériser *leurs propres outils militaires* en vue d'effets opérationnels précis, centrés sur les adversaires qui cherchent à les combattre. Numériser les forces armées ne va pas sans une réflexion approfondie sur la répartition des tâches entre armée, police et renseignement, ainsi que, bien entendu, sur le partage des informations entre ces trois entités. Cela implique, même si cette piste est à contre-courant des discours imposés depuis 2008 au sujet du continuum défense-sécurité, de distinguer sans les disjoindre les tâches de la défense et celle de la sécurité.

La vision *extensive* de la cybermenace ou de la cyber-conflictualité constitue sûrement une stratégie d'argumentation pertinente pour convaincre les hiérarchies en place de consacrer des crédits substantiels aux nouvelles technologies, qui ont pu paraître à leur début comme de simples « gadgets » face aux armes traditionnelles ou « cinétiques ». Cette manière de présenter sous un jour inquiétant le potentiel d'hostilité de la numérisation de l'économie auprès des décideurs politiques et de l'opinion publique a certainement été utile à l'intérieur du jeu des bureaucraties concurrentes, pour se voir allouer une part jugée satisfaisante du budget étatique[38].

Malgré ces justifications ponctuelles et parfaitement classiques du point de vue de l'analyse politique, il semble qu'il soit aujourd'hui urgent de reformuler la nature 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[39], en particulier depuis l'instauration du COMCYBER, sur lequel nous reviendrons. Notons simplement que ce dernier a été positionné au sein même de l'État-Major des Armées, et non comme une « 4e armée ».

Le terme « cyber » appartient à un autre âge de l'épopée informatique. Comme d'autres mots-valises encore plus anciens (qui utilise encore « technotronique », très en vogue dans les années 1970 ?), il pourrait être pertinent de l'abandonner au moins sous sa forme de préfixe fourre-tout et englobant. Personne ne dirait plus aujourd'hui que Google ou Apple sont des « cyber-entreprises » ou qu'elles œuvrent « dans le cyber ». Ce sont des entreprises de technologie numériques et informatiques, qui inventent et vendent de nouvelles manières d'acquérir, traiter et communiquer les données informatiques[40]. Il s'agit là très

[36] Cf Deptula « Mosaic Warfare », op. cit. 2019, p.22.
[37] Terme très souvent employé dans le Livre Blanc de 2013.
[38] C'est ce l'on peut observer en France avec la distribution des rôles entre la DGSE, l'ANSSI et le ComCyber, qui dépendent respectivement de la branche renseignement du Ministère des Armées, du Premier Ministre et du SGDSN pour le second et enfin de l'Etat-Major des Armées pour le Commandement des Forces Cyber.
[39] Iasiello, Emilio, "Are Cyber Weapons Effective Military Tools?" in *Military & Strategic Affairs*, vol.7, n° 1, mars 2015.
[40] Autre terme très en vogue dans les années 1980, la « télématique », terme né de la contraction de *télécommunication* et d'*informatique* sous la plume de Simon Nora et d'Alain Minc, dans un rapport remarqué, rédigé en 1978 à propos de « l'informatisation de la société ». Associé à l'ère du Minitel, le mot a totalement disparu avec l'avènement d'Internet et la disparition du terminal français en 2001. Voir Mathelot, Pierre, *La Télématique*, Paris, PUF, coll. « Que sais-je ? », 1982. On peut interpréter la disparition du terme comme une conséquence de l'absence d'anticipation d'un réseau

précisément d'une tâche dont les armées doivent s'acquitter dans la mission qui leur a été confiée, à savoir défendre les intérêts français par la force lorsque des groupes les menacent au travers de revendications politiques violentes. Le reste est du ressort de la police, lorsqu'il s'agit de délinquance, et des services de renseignement non-militaires lorsqu'il s'agit de menaces d'usage potentiel de la violence (par exemple l'interception de groupes terroristes) et d'activités mettant en péril l'intérêt national. Reste à mettre au point une méthode permettant de calculer les coûts et les bénéfices de l'implantation d'ensembles techniques numériques au sein des systèmes d'armes actuels.

Multiplicité des modèles de numérisation : intégration numérique et *path dependence*

L'intégration numérique des armées peut être définie plus exactement comme le resserrement de tous les niveaux et de tous les milieux de la guerre, de manière à faire combattre les composantes des armées d'une manière plus coordonnée que tout ce qui était auparavant imaginable avec des systèmes analogiques. Il ne s'agit pas, dans la perspective de cette note, de diagnostiquer la naissance d'un nouvel espace, mais bien d'apprécier les conséquences de la formation d'un ensemble transversal d'outils techniques, permettant de mieux « ligaturer » les milieux où se déroulent les affrontements et de mieux coordonner les manœuvres. C'est précisément cette nouvelle forme d'intégration que l'on nomme actuellement « opérations multidomaine » dans les documents de doctrine officiels américains et français[41], même si ce vocable recouvre encore pour le moment des acceptions très variées. Toutes les propriétés émergentes de cette intrication inédite des différents milieux (ou « domaines ») stratégiques ne sont pas encore explorées et seront sans aucun doute possible la source des prochaines « surprises stratégiques »[42].

Pour être efficaces, de tels systèmes de communication et de coordination ne doivent pas seulement suivre une logique technique qui en ferait des outils inadaptés aux besoins militaires concrets. Un des principaux défis de la réussite de leur implantation réside donc dans leur cohérence avec le modèle d'armée sur lequel cet « ensemble technique »[43] est greffé. Il n'existe donc pas « un » modèle unique à suivre, mais une multiplicité de solutions dont la meilleure sera celle qui répondra à une triple nécessité :

- combattre plus efficacement ;
- sécuriser le nouveau système ;
- réduire le coût et la durée de la transformation[44].

In fine, la transition vers un modèle technique numérique doit donc permettre aux armées d'améliorer leurs fonctions de combat, en s'assurant de faire apparaître le moins de vulnérabilités numériques possible et en optimisant le « coût de transaction » induit[45].

Le défi de la numérisation de l'appareil militaire vise à adapter au mieux les nouvelles technologies aux systèmes militaires existants. Une piste serait

ouvert et totalement décentralisé, auquel il est possible de se connecter grâce à plusieurs types de terminaux. C'est l'inverse de la vision technique du Minitel, réseau fermé, centralisé, et auquel on ne pouvait accéder qu'à l'aide d'un seul appareil, qui n'a que très peu évolué en vingt ans d'existence. De ce point de vue, le terme « cyber » correspondait mieux à l'ère d'internet que celui de « télématique ».

[41] Voir le document où a été officiellement dévoilé le concept : *FM 3.0, Operations*, Washington, Headquarters Department of the Army, Octobre 2017.

[42] Bott, Jonathan W., "What's After Joint? Multi-Domain Operations as the Next Evolution in Warfare", United States Air Force School of Advanced Military Studies, Fort Leavenworth, 2017. Voir aussi le document de doctrine officiel de l'Armée de Terre française, *L'emploi des forces terrestres dans les opérations interarmées* (DFT 3.2 Tome 1 [FT-03]), 1er juillet 2015. On y parle de « coordination interdomaine » (p.35), permise par le numérique.

[43] Tous les concepts entre guillemets sont empruntés à Gilbert Simondon et à son ouvrage classique *Du Mode d'existence des objets techniques*, Paris, Aubier-Montaigne, 1958.

[44] "Strategic Cyberspace Operations Guide", *United States Army War College*, Carlisle, Pennsylvania, juin 2016.

[45] Selon le concept de Ronald Coase dans *The Nature of the Firm* (1937), qui lui valut 54 ans plus tard le Prix Nobel d'Economie. La théorie économique considère les coûts de « policing and enforcement » comme des coûts de transaction. Cf Dahlman, Carl J., "The Problem of Externality" in *Journal of Law AMD Economics,* n° 22, vol.1, 1979, pp.141–162.

de partir de l'expérience concrète des utilisateurs du produit fini (l'*user experience*, c'est-à-dire les militaires eux-mêmes) afin que la technologie mise en place pour accomplir une tâche précise maximise réellement les nouvelles possibilités opérationnelles tout en minimisant le « coût de transaction » (c'est-à-dire, dans le cas qui nous occupe, la quantité d'énergie nécessaire à la mise en place et à l'apprentissage des nouvelles techniques). Pour envisager ce phénomène, il est sans doute nécessaire de garder à l'esprit que la numérisation et la mise en réseau des forces est soumise, à l'inverse de ce que l'on pourrait croire intuitivement, à un très puissant effet de *path dependance*. Le coût des nouvelles technologies doit être évalué à partir du « coût de transition » depuis l'état antérieur du système, et notamment du coût cognitif pour les utilisateurs finaux, c'est-à-dire les militaires[46].

Pour être plus précis encore, nous pourrions dire que l'imposition d'un nouvel « ensemble technique » numérique de communication et d'incorporation des « éléments » et « individus techniques »[47] à l'intérieur des ensembles préexistants est nécessairement incrémental. Il doit par conséquent prendre en considération leurs caractéristiques et leurs limites afin de pouvoir définir une stratégie de transformation maximisant les améliorations, mais sans faire exploser les coûts. C'est ce que les armées appellent le *retrofit*, ou ajout de nouvelles technologies à d'anciens matériels. La quantité d'efforts à fournir pour faire transiter le système d'un état à un autre conditionne ainsi le degré d'agilité et de versatilité numérique et technique des armées. Une meilleure prise en compte de ces paramètres dans la phase de préparation de la numérisation d'une unité pourrait ainsi permettre un gain de temps et d'efficacité. La réduction du coût de transaction par celle du cycle de conception pourrait ainsi être atteint grâce à l'adoption d'un modèle de développement plus agile, « en spirale »[48], intégrant d'emblée l'*user experience*.

Exemple très caractéristique, la modernisation des B-52 américains et des Tupolev-95 russes a eu pour résultat une modernisation du système de navigation grâce à de nouveaux outils (« individus » dans le langage de Simondon). Conçus dans les années 50, ces deux modèles de bombardiers nucléaires à long rayon d'action ont été « numérisés » et connectés au système technique de leurs armées respectives grâce à un nouveau système de transmission numérique, bien différent de celui, analogique, du Strategic Air Command. Un autre exemple pertinent serait ici celui des chars Abrams M1, constamment *upgradés* depuis leur mise en service en 1981. La dernière mise à jour, nommée M1A2, concerne l'implantation de systèmes de contrôle et de communication numériques et cherche à doter ce char au moteur et à la conception très robustes des moyens de participer pleinement à la bataille numérisée à venir, sans pour autant envoyer à la casse les centaines d'exemplaires dont dispose l'armée américaine[49].

Pareillement, le programme SCORPION de modernisation des véhicules blindés de l'Armée de Terre française comporte un *retrofit* des chars Leclerc, dans une version baptisée XLR. Les engins blindés, entrés en service en 1997 se verront ajouter de toutes nouvelles capacités de communication cryptées : le Système d'Information de Combat

---

[46] Kurti, Erdelina & Haftor, Darek, "The Role of Path Dependence in the business model adaptation: from traditional to digital models", Proceedings of the 2014 Mediterranean Conference on Information Systems, Paper 28. Notons que l'on ne doit également pas surévaluer ces coûts, en choisissant des technologies trop simples, adaptées aux soldats d'aujourd'hui, mais qui seront insuffisantes pour les générations qui arriveront lors des prochains recrutements (la vitesse de rotation des effectifs étant d'ailleurs plus rapide dans les armées que dans une entreprise).

[47] Gilbert Simondon, *Du Mode d'existence des objets techniques*, *op. cit.*

[48] Cf Boehm, Barry, "A Spiral Model of Software Development and Enhancement", in *ACM SIGSOFT Software Engineering Notes*, ACM, n° 11, vol.4, pp.14-24, août 1986. Le modèle de développement en spirale, fondé sur l'expérimentation précoce et le prototypage, est d'ailleurs né dans la gestion de projets complexes dans le domaine informatique et de la mise au point de logiciels.

[49] Gouré, Daniel, "The M1A2 Abrams Is The Tank Of The Future", *The National Interest*, 3 novembre 2018 (https://nationalinterest.org/blog/buzz/m1a2-abrams-tank-future-35067?fbclid=IwAR3s0r7COu77roRCQcMsanovowdslEskkp0BnwfSVDvvBnQ7EymF2IUah8s)

Scorpion (SICS) et Vétronique, qui lui permettront de communiquer avec les autres véhicules de la nouvelle gamme (Griffon, Serval, Jaguar) de manière sécurisée. Une telle démarche correspond aux concepts complémentaires que l'Armée de Terre désigne par les termes d'« info-valorisation » et de « combat collaboratif »[50].

Conceptuellement distincts, ces deux objectifs visent pour l'une la production d'une connaissance sous forme de donnée, pour l'un, et une amélioration de la manœuvre pour l'autre. Ils dépendent cependant, *in fine*, de la qualité de la captation et de la transmission des informations numérisées et donc de l'efficience de l'architecture de données. L'art opératif est-il pour autant devenu une simple fonction de la qualité des outils numériques ? Bien au contraire, c'est la qualité des outils numériques qui se mesurent aux possibilités de manœuvre et de commandement qu'ils permettent. La possibilité de commander avec un certain degré de liberté doit donc être pensée et intégrée dès la conception de l'objet technique numérique militaire.

Ainsi, l'une des principales limitations actuelles est l'insuffisance de la bande passante permettant l'échange de données dans le circuit capteur/C2/effecteur, souvent saturé sur des systèmes pensés avant l'an 2000. Le système d'Information de Combat Scorpion (SICS) bénéficie dans cette perspective d'un élargissement de bande passante, afin de pouvoir faire transiter un volume de données suffisant. Ceci permet précisément une intégration tactique plus serrée, tout en rendant plus aisé le *Command & Control* des chars, avec notamment une acquisition de cible partagée. Libérée d'une contrainte technique, la manœuvre gagne en agilité, en rapidité d'exécution et en imprévisibilité.

L'Armée de Terre attend ainsi de cette refonte un réel gain de puissance de la mise à jour de son *système de communication et de coordination numérique*. À titre d'exemple, celui dont bénéficieront les blindés intégrés à Scorpion baptisé Synthèse Tactique (SYNTAC), permettra « une vision cartographiée partagée de l'environnement et de l'adversaire et au travers de la réalité augmentée »[51]. Jouant pleinement la carte de l'innovation et du partage d'informations, certaines versions pourraient même abriter des drones de reconnaissance permettant d'augmenter la visibilité sur le champ de bataille afin de faire parvenir les données recueillies avec les unités plus fragiles devant rester plus loin du front[52]. Le même nombre de blindés sera ainsi en mesure de produire davantage de puissance grâce à la concentration des feux découlant du SYNTAC, tout en conservant une dispersion physique limitant la vulnérabilité. C'est là un cas d'école d'incorporation et de conjonction numériques, fondé sur le *retrofit* d'anciens matériels et l'ajout incrémental de nouveaux éléments au sein d'un système technique repensé pour la mise en commun de l'information.

Problèmes et dilemme de la numérisation de l'espace de bataille

Cette intégration numérique poussée est le fruit d'une réflexion engagée depuis plusieurs années, notamment depuis le Livre Blanc de 2008. L'outil militaire français a lui aussi été mis au défi par le progrès très rapide de la numérisation, dans un contexte budgétaire tendu, caractérisé par une baisse constante des budgets depuis la fin de la Guerre froide, jusqu'au choc des attentats de 2015. Le problème de l'introduction d'un système numérique de communication et de coordination[53] était

[50] Cf Paul, Philippe, « Notions sur le combat collaboratif et observations récentes des expérimentations », in *Pensée Mili-Terre*, Paris Centre de Doctrine et d'Enseignement du commandement, juin 2019, p.1.

[51] *Ibid.*, p.2.

[52] Lagneau, Laurent, « Nexter prépare une version du char Leclerc capable de mettre en œuvre des drones aériens », in *Zone Militaire* 21 février 2019. http://www.opex360.com/2019/02/21/nexter-prepare-une-version-du-char-leclerc-capable-de-mettre-en-oeuvre-des-drones-aeriens/.

[53] Equivalent pour l'armée des systèmes SCADA (d'acquisition et de contrôle à distance des données) utilisés dans l'industrie, permettant de monitorer un ensemble complexe d'objets techniques inertes. La différence pour l'armée est qu'elle doit contrôler des êtres animés et autonomes, faisant face à des ennemis eux-mêmes autonomes et inventifs. Les deux activités ne peuvent donc être pensées avec le même cadre conceptuel.

déjà soulevé dans les Livres Blancs de 2008 et de 2013 et a de nouveau été abordé dans la Revue Stratégique parue en octobre 2017[54].

Pionnier dans la formulation d'une stratégie numérique, le Livre Blanc de 2008 invoquait le concept de « Lutte informatique offensive (LIO) », devant permettre à la France de répliquer aux attaques numériques. Surtout, il proposait, 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. *« L'efficacité à tous niveaux des forces de défense et de sécurité dépend et dépendra de plus en plus du bon fonctionnement de leurs systèmes d'information, avançait le LBDSN de 2008. 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 système de défense pourra être […] désorganisé et partiellement aveuglé au travers de frappes silencieuses et ciblées* »[55].

On notera ici l'abandon précoce du préfixe cyber- pour décrire ces opérations, qui ne sont pas du tout « virtuelles », puisqu'elles participent directement à l'effort militaire et ont pour objectif de minimiser le danger auquel font face les soldats. Les problèmes techniques d'une telle implantation de capacités de combat numériques étaient déjà évoqués, mais sans aborder la question du commandement effectif de ces missions. Même si l'intrication était vue comme nécessaire, l'idée d'une contribution directe aux forces « dans le dernier kilomètre tactique » n'était pas encore abordée.

Le Livre Blanc de 2013 insistait quant à lui beaucoup sur la constitution d'une « cybermenace », et évoquait plus distinctement l'idée d'une intégration des capacités numériques aux forces armées. Discriminant bien ce qui est du domaine de la délinquance et de la mission de protection de l'État, il posait le constat de l'interdépendance des certains intérêts privés et de ceux de la communauté politique et donnait en conséquence une version *extensive* de la tâche des armées : « *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* »[56].

Bien que la menace informatique soit ici séparée d'une partie relevant des services de police, la « cybermenace » continue de constituer un domaine extrêmement large. La véritable modification tactique et opérationnelle induite par les nouvelles capacités de diffusion de l'information n'était pas analysée en soi, mais au travers de la connexion entre renseignements et états-majors. Ancrée dans la « théorie des cinq milieux » (terre, air, mer, espace extra-atmosphérique et « cyberespace »), la réflexion stratégique française bute ainsi sur la définition d'objectifs relatifs à l'introduction des nouveaux outils numériques au sein même de l'espace de bataille constitué par les quatre milieux qu'irrigue en réalité le « cyber ». Elle cantonne la mission à la volonté d'« *[…] acquérir et de conserver la supériorité opérationnelle sur nos adversaires* »[57] et précise que les « engagements de coercition »[58] doivent être « *conduits de façon coordonnée dans les cinq milieux* »[59]. Une

[54] *Revue Stratégique*, Paris, Secrétariat Général à la Défense et à la Sécurité Nationale, 2017, notamment dans la partie 1, titre 4, « Des ruptures technologiques et numériques », pp.33-37. Pour le problème de la numérisation des armées dans la Revue Stratégique, voir *infra*.

[55] *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.

[56] Livre Blanc de la Défense et de la sécurité Nationale de 2013, p.45.

[57] *Ibid.*, p.84.

[58] *Ibid.*

[59] *Ibid.*

telle vision suppose, dans une démarche que l'on peut qualifier de mahanienne, la constitution de forces propres au nouveau « domaine », sur le modèle de la Marine et de l'Armée de l'Air, bien séparées budgétairement et hiérarchiquement de l'Armée de Terre.

Toutefois, il est permis de penser que la création d'une « 4e armée cyber » n'est pas la voie appropriée[60]. Il n'est en effet nullement possible de comparer le domaine aérien ou maritime 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 » entièrement nouveau s'adaptant à tous les autres milieux et pouvant être déployé partout, tandis que les autres milieux restent nettement séparés.

La question du commandement affleurait cependant dans le Livre Blanc de 2013. Elle révèle à ce moment précis du débat stratégique français une véritable tension intellectuelle entre les tenants d'un milieu à part entière et ceux d'une meilleure intégration et synchronisation des forces armées grâce 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, pose le document à l'époque. 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* »[61]. 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* »[62].

C'est à l'aune de ces conceptions doctrinales qu'il faut apprécier les changements survenus dans l'organisation des forces armées depuis une dizaine d'années. Tous vont dans le sens d'une intrication numérique des diverses unités et d'une collecte et d'une transmission de plus en plus rapides de l'information entre unités, plutôt que dans le sens d'une « 4e armée cyber », venant s'ajouter organiquement à l'Armée de Terre, la Marine et l'Armée de l'Air, comme nous allons le voir à présent.

Le défi organisationnel et humain de la numérisation

La France s'est peu à peu dotée de moyens institutionnels pour assurer sa sécurité numérique, menacée par la multiplication d'actions hostiles menées par les acteurs transpolitiques protéiformes renforcés par la nouvelle agorie numérique militaire. L'identification des nouvelles menaces a tout d'abord eu pour conséquence la création de nouvelles structures encadrant l'effort de sécurité dans le domaine informatique, telles que l'ANSSI en 2009, ou la réserve citoyenne de cyberdéfense en 2012. On y ajoutera le « COMmandement des Systèmes d'Information et de Communication » (abrégé en COMSIC), placé sous la houlette d'un unique officier, et comptant dans ses rangs 4 750 militaires et 150 civils[63], la 807e brigade CTRS (spécialisée dans les transmissions), ainsi que la réserve opérationnelle de cyberdéfense en 2016. Enfin, le COMCYBER (« COMmandement cyber), qui coiffe l'ensemble des dispositifs numériques au sein des trois armées, est implanté en janvier 2017 au sein même de l'État-Major des Armées, écartant donc la création d'une armée spécifique.

[60] Gartzke, Erik, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth" in International, Security, vol. 38, N° 2, automne 2013, pp.41–73. Singer, Peter & Shachtman, Noah, "The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive", Brookings.com, 15 aout 2011.

[61] Livre Blanc de la Défense et de la sécurité Nationale de 2013, p.94. Nous soulignons.

[62] *Ibid.*

[63] Dossier « L'armée de Terre Au Contact », Juillet-Août 2016, Ministère de la Défense.

La mission du COMCYBER révèle de manière parfaitement claire que l'organisation des forces numériques n'aboutira sans doute pas à la création d'une entité séparée. Bien au contraire, celui-ci a pour tâche de coordonner, sous l'autorité directe du Chef d'État-Major des Armées l'ensemble de l'action numérique des armées. Son implantation au cœur même des services centraux de commandement des armées (sur le modèle du CYBERCOM américain, créé en 2010 et intégré au *Joint Commandement)* montre de manière évidente que l'on a préféré le placer au point nodal de la prise de décision, plutôt que de créer une structure complète qui aurait encore alourdi le processus de coordination. Dans cette optique, les services et les ressources informatiques sont au service de toutes les unités de l'armée et de toutes les armes, tout en leur permettant de disposer des renseignements les plus précis possible pour définir leurs cibles, parer ou éviter un éventuel coup de l'adversaire et guider les opérations « cinétiques » de manière plus rapide et plus réactive, c'est-à-dire nécessitant l'emploi de la force physique.

L'emploi de moyens numériques ne se cantonne donc absolument pas à un espace séparé et indépendant, mais pèse de tout son poids sur la conduite de la guerre. La Revue Stratégique, publiée en octobre 2017, insiste particulièrement sur ce point. Adoptant l'esprit de l'intégration cyber-tactique, elle éloigne encore un peu plus l'armée française de la vision cyber-espace/cyber-stratégie/cyber-armée : « *Les armées*, précise le document, *doivent […] 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* »[64].

Ce document est complété six mois plus tard par la *Revue Stratégique de Cyberdéfense*[65], qui vient définir les rôles en termes de surveillance de la menace et de réaction aux actions malveillantes, afin de doter l'État français d'une politique globale cohérente en matière de sécurité numérique. Centrée sur la protection des services vitaux de la nation, cette première revue spécialisée dans le domaine numérique acte la tripartition des rôles entre du Renseignement non-militaire (la DGSI), le Ministère des Armées (le ComCyber, implanté au sein de l'Etat-Major des Armées) et l'exécutif (l'ANSSI dépend du SGDSN, organisme directement subordonné au Premier Ministre)[66].

Du point de vue de la science politique et du « partage du pouvoir » entre bureaucraties concurrentes, le morcellement de l'autorité entre plusieurs organismes dépendant d'autorités différenciées semble donc entériné. Rédigée par le SGDSN, la revue souligne « le rôle normatif de l'ANSSI », l'une de ses composantes, dont le rôle est précisé et affirmé un an après la création du ComCyber[67].

Découlant directement des recommandations portées dans ces deux « revues stratégiques », un double document est publié par le Ministère des Armées en janvier 2019, précisant l'usage militaire des moyens numériques. Dans ses parties respectivement intitulées « Éléments publics de doctrine militaire de lutte informatique offensive » et « Éléments publics de doctrine militaire de lutte informatique défensive »[68], ce double document

[64] *Revue Stratégique*, Paris, Secrétariat Général à la Défense et à la Sécurité Nationale, 2017, §299, p.83.

[65] *Revue Stratégique de Cyberdéfense*, Paris, Secrétariat Général à la Défense et à la Sécurité Nationale, 2018.

[66] *Ibid.* pp.46-47.

[67] Voir notamment p.108 : « *Forte de sa mission et de ses compétences, l'ANSSI s'est naturellement imposée comme référent pour la définition des normes de sécurité pertinentes pour assurer la protection des données et des systèmes d'information les plus sensibles, à commencer par la protection du secret de la défense nationale* ».

[68] *Éléments publics de doctrine militaire de lutte informatique offensive* & *Éléments publics de doctrine militaire de lutte informatique défensive*, Paris, Ministère des Armées, janvier 2019, https://www.defense.gouv.fr/salle-de-presse/communiques/communique_la-france-se-dote-d-une-doctrine-militaire-offensive-dans-le-cyberespace-et-renforce-sa-politique-de-lutte-informatique-defensive

dote la France de règles d'engagement (*rules of engagement*, souvent abrégé ROE) clarifiées, procurant aux agents français des directives précises sur ce qui est leur permis. Une répartition des rôles est également établie, afin de ne pas souffrir d'hésitations et de débats nuisibles dans les moments où l'action doit être rapide et décidée, notamment en temps de crise aigüe. Surtout, on peut y lire la manière dont est envisagée l'organisation générale de la manœuvre numérique, ainsi que son niveau *d'intégration* avec l'action militaire prise dans un sens extensif.

La doctrine offensive souligne tout d'abord l'existence de « champs d'actions possibles » pour les attaquants, dont « les quatre objectifs majeurs sont l'espionnage, les trafics illicites, la déstabilisation et le sabotage »[69]. On note qu'il n'est nullement question d'action militaire, mais de continuation numérique d'actions illicites.

Le document défensif précise que « *le cyberespace est un milieu de confrontation pour les États ou les organisations non gouvernementales dans lequel le risque d'attaque est considéré comme permanent, y compris en temps de paix* »[70].

Distingué dans la Revue de Cyberdéfense[71], La Lutte Informatique Offensive (LIO) et Défensive (LID) reçoivent des définitions précises :

- « *La lutte informatique offensive à des fins militaires (LIO) recouvre l'ensemble des actions entreprises dans le cyber-espace, conduites de façon autonome ou en combinaison des moyens militaires conventionnels. [Elle] vise à produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité ou la confidentialité des données* »[72].
- La lutte Défensive, quant à elle, est plus vaste et déborde largement le domaine militaire. « *La LID regroupe l'ensemble des actions, techniques et non techniques, conduites pour faire face à un risque, une menace ou à une cyberattaque réelle, en vue de préserver notre liberté d'action. La LID couvre principalement trois de ces missions : anticiper, détecter et réagir et complète les missions : prévenir, protéger et attribuer. Elle contribue ainsi à la résilience des armées et plus globalement à l'élaboration des stratégies de réponse aux niveaux ministériel et interministériel* »[73]. Sa conception et son exécution sont par nature interministériel et, par conséquent, dépassent le champ de compétence de l'Etat-Major des Armées ou du Ministère des Armées.

Du point de vue opérationnel, la LIO est la seule pertinente dans la conception et la mise en place d'une action sur un théâtre de guerre. Par conséquent, celle-ci « *[…] se conçoit aux niveaux stratégique (dans la manœuvre opérationnelle interarmées globale) et tactique (dans la manœuvre des composantes d'armées sur les théâtres d'opérations)* »[74].

La constitution d'une manœuvre numérique, ou la participation à une manœuvre globale, supposent à la fois un degré d'autonomie permettant la mise au point d'opérations possédant de nombreux traits distinctifs, et la maîtrise d'un niveau de coordination suffisant pour assurer la *conjonction stratégique*. *« L'emploi de la LIO*, insiste donc le document, *s'inscrit dans une temporalité qui lui est propre. Si ses effets peuvent être fulgurants, son intégration dans la manœuvre opérationnelle globale est un processus qui se caractérise par une planification longue et très spécifique. Ces effets peuvent être d'ordre matériel – neutralisation d'un système d'arme – ou immatériel – collecte de renseignements temporaires, réversibles ou définitifs. [Elle] propose des modes d'action discrets et efficaces contre les systèmes numérisés, capables de se*

[69] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, p.4.
[70] *Éléments publics de doctrine militaire de lutte informatique défensive*, *op. cit.*, p.9
[71] *Revue Stratégique de Cyberdéfense*, *op. cit*, p.52
[72] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, p.5.
[73] *Éléments publics de doctrine militaire de lutte informatique défensive*, *op. cit.*, p.5.
[74] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, p.7.

substituer à d'autres modes d'action, de les préparer ou les compléter »[75].

Pour ce qui est de l'*intégration tactique numérique*, la doctrine offensive retient « *trois types d'objectifs opérationnels dans la conduite d'opérations militaires :*

1) Évaluation de capacités militaires adverses : recueil ou extraction d'informations ;

2) Réduction voire neutralisation de capacités adverses : perturbation temporaire ou création de dommages majeurs dans les capacités militaires adverses ;

3) *Modification des perceptions ou de la capacité d'analyse de l'adversaire : altération discrète de données ou systèmes, exploitation d'informations dérobées au sein d'un système d'information militaire de l'adversaire* ».

Il se constitue donc ici des capacités de renseignement, de sabotage, de propagande ou de désinformation. Ces opérations sont conduites en toute indépendance par les militaires et sont placées « *sous l'autorité du chef d'état-major des armées* »[76]. Ainsi, « *le COMCYBER*[77] *est l'autorité d'emploi de la capacité militaire cyber offensive, partie intégrante de la chaîne opérationnelle des armées, en parfaite cohérence avec leur organisation et leur structure opérationnelle* »[78]. Ceci a pour objectif d'assurer la parfaite conjonction stratégique des forces et de ne pas multiplier les chaînes de commandement pouvant avoir des objectifs dissemblables.

Cependant, cette nécessaire autonomie numérique de l'Etat-Major des Armées implique une maitrise totale de ses propres capacités informatiques. Ne peut-on voir ici une contradiction avec la compétence générale de l'ANSSI sur la sécurité informatique des ministères et des agences de l'État ? C'est sans doute pour dissiper tout malentendu que la Revue Stratégique de Cyberdéfense de 2018 a conçu quatre « chaines opérationnelles », définissant des domaines de compétence. Ainsi, une chaîne « action militaire » est confiée au Ministère des Armées et se distingue des chaînes « renseignement », « investigation judiciaire » et « protection »[79]. Là encore, le partage des rôles, déjà effectif dans les faits, est entériné par la publication d'un document de doctrine venant consolider une situation existant déjà *de facto*.

Néanmoins, certaines actions, situées aux confins entre ces quatre domaines, nécessitent ponctuellement une collaboration de l'ensemble des acteurs. Comment, en effet, déléguer à un seul acteur la lutte contre les flux financiers illégaux venant abreuver les groupes insurgés islamistes au Sahel, contre lesquels la France lutte ? Comment répondre à une attaque de l'État Islamique sur une chaîne d'information ou un journal français, menacés de perdre l'ensemble de leurs données et n'ayant plus la maîtrise du contenu qu'ils diffusent (comme cela a été le cas en 2015 pour TV 5 Monde et pour le compte Twitter du journal Le Monde[80]) ? Ainsi, afin d'assurer la cohérence et la coopération de l'ensemble de ces chaînes opérationnelles, un *Centre de coordination interministériel des crises cyber* est instauré en avril 2018. Celui-ci est *« animé par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) sous l'autorité du Premier ministre* »[81]. Quatre domaines y sont traités de manière distincte : « *protection, action militaire, renseignement et investigation judiciaire* »[82].

L'analyse, fastidieuse mais nécessaire, de la mise en place progressive de ces différentes doctrines, montre que la France a consolidé un modèle

---

[75] *Ibid.*, p.6.
[76] *Ibid.*, p.6.
[77] Rattaché, rappelons-le, au Chef d'Etat-Major des Armées.
[78] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, *p.5*
[79] *Revue Stratégique de Cyberdéfense*, *op. cit*, p.53.
[80] Cf Boyer, Bertrand, « Comprendre les cyber-opérations », essai auto-publié (https://www.amazon.fr/gp/product/B0173TUS0W/ref=dbs_a_def_rwt_hsch_vapi_tkin_p1_i0), et l'article de Damien Leloup et Untersinger, Martin, « Comment notre compte Twitter a été piraté », *Le Monde*, 24 janvier 2015.
[81] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, p.4.
[82] *Ibid.*

de lutte informatique reposant, en dernière instance, sur l'exécutif, en collaboration étroite avec l'état-major interarmées et le renseignement, et non exclusivement sur ces derniers (c'est là une différence notable avec le modèle américain, où le poids et la spécificité d'une agence comme la NSA induit des interactions différentes entre acteurs bureaucratiques de la lutte informatique). Notamment dans le domaine offensif, l'autorité militaire affirme dans son document de doctrine sa totale autonomie : « *Les actions de LIO sont conduites, sous la responsabilité du chef d'état-major des armées, dans le cadre défini en droit interne par le code de la défense et dans les conditions fixées par le Premier ministre* »[83].

Ainsi se dégage peu à peu une politique globale d'intégration numérique, prolongeant la doctrine dite de Posture Permanente de Sûreté (PPS) vis-à-vis des menaces nées de la généralisation des communications informatiques à distance : « *La tension générée par ces attaques cyber, cycliques ou soudaines, de gravités variables, impose l'adoption d'une vigilance de tous les instants, qui s'incarne à travers la posture permanente de cyberdéfense (PPC) pour le ministère des Armées. La PPC est constituée de l'ensemble des dispositions adoptées pour assurer en permanence (24h/7j) la défense des systèmes informatiques du ministère dans le continuum paix-crise-guerre* »[84].

[83] *Éléments publics de doctrine militaire de lutte informatique offensive*, *op. cit.*, p.10.

[84] *Éléments publics de doctrine militaire de lutte informatique défensive*, *op. cit.*, p.9.

Pour assurer une défense de ses serveurs et de ses outils de lutte numérique, le Ministère s'est également doté d'organisations propres consacrées à cette tâche : « *A l'échelle du ministère, sous les ordres du COMCYBER, le Centre d'analyse en lutte informatique défensive (CALID) assure une "hypervision" technique d'ensemble, qui synthétise et partage l'information des situations cyber produites par l'ensemble des* Security Operating Centers *ou par ses moyens propres* »[85]. Par les derniers documents publiés, le Chef d'Etat-Major des Armées renforce son rôle et écarte toute contestation possible de son autorité dans la « chaîne militaire » créée par la Revue Stratégique de Cyberdéfense : « *Au sommet de la chaîne de LID, le COMCYBER s'appuie sur le centre des opérations cyber (CO Cyber) pour orienter le travail du CALID et des* Security Operating Centers*. En particulier, il partage l'état de la menace cyber et des nouvelles vulnérabilités découvertes afin d'optimiser l'efficacité de la chaîne de cyberdéfense et de protection du ministère* »[86].

Ne pouvant néanmoins être assurée en permanence par les forces armées, cette posture défensive permanente est assurée en temps routinier par l'Agence nationale de Sécurité des Services Informatiques, mais peut basculer à tout moment en configuration de crise, afin de pouvoir opérer en

Exercice Serpentex 2016, Appui aérien rapproché assisté par l'emploi d'outils numériques
Image : Assemblée nationale, Commission Défense

[85] *Ibid.*, p.8.

[86] *Ibid.*

coordination avec les forces armées et les agences de renseignement. Les risques d'ambiguïté dans la définition de compétence dans les instants décisifs d'une crise ou de refus de partage d'information ont de ce fait été réduits. L'État français s'est ainsi donné progressivement les moyens d'instaurer une forme de déconfliction au sein de sa politique de défense numérique dès la parution du Livre Blanc de la Défense de 2008 et la création des premières agences dédiées, concurremment à la mise en place de services spécialisés au sein des armées et des services de renseignement.

Il est ainsi affirmé que la mission défensive « *incombe à l'Agence nationale de sécurité des systèmes d'information (ANSSI), en coordination avec les services de renseignement et le Commandement de la cyberdéfense (COMCYBER) sur le périmètre du ministère des Armées* »[87]. La « mission de cyber défense » de « réaction »[88], reçoit ainsi un cadre et une définition précise : « *il s'agit de résister à une cyberattaque afin qu'elle n'empêche pas la poursuite de notre activité. Dans la plupart des cas, le COMCYBER déclenche alors une opération de LID, en liaison avec l'ANSSI. Elle peut entraîner l'emploi de moyens qui sortent du domaine de la cyberdéfense, voire du ministère des Armées (saisie de la justice, action diplomatique, rétorsion économique, etc.)* »[89].

Enfin, la responsabilité ultime, qui est celle de tirer les conséquences politiques d'une attaque numérique, reste la prérogative du chef de l'État : « *Les services de renseignement sont au cœur de ce processus de recueil d'indices d'attribution. La décision d'attribution appartient aux plus hauts responsables politiques* »[90].

Notons que l'attribution de la responsabilité d'une attaque à un État reconnu diplomatiquement, soit comme opérateur direct, soit comme sponsor, vient de recevoir une réponse originale dans la doctrine américaine. Tout Etat accusé d'attaque informatique, sponsorisant une attaque ou bien abritant un groupe organisant une telle offensive mettant en danger la sécurité nationale, sera justiciable d'une riposte non pas simplement symétrique et limitée au domaine de la lutte numérique, mais « cinétique ». En cela, les États-Unis ont officiellement étendu le champ de la dissuasion conventionnelle et non-conventionnelle au domaine numérique. Tout État utilisant activement ou passivement la déstabilisation informatique est ainsi menacé d'une frappe militaire semblable à celle qu'entraînerait l'emploi des forces traditionnelles[91]. Ceci représente une extension du principe du *peace through strength* par rapport à laquelle la France ne pourra manquer de se positionner dans les années à venir.

L'ultime étape : la numérisation du « dernier kilomètre tactique »

Au travers d'un commentaire des derniers documents de doctrine publiés, nous venons d'examiner en détail la stratégie globale de la France afin de se doter d'institutions englobantes, permettant de faire face à des attaques générales, ressortissant exclusivement du domaine numérique. Mais qu'en est-il de la numérisation des unités traditionnelles, devant mettre en place des moyens de lutte informatique offensive ou défensive ?

Pour cela, l'architecture numérique examinée ci-dessus est un préalable nécessaire, mais n'est pas le fin mot de la réforme numérique des armées. Beaucoup d'actions sont mineures ou bien ne peuvent, sur le terrain, attendre que soit respecté le délai nécessaire à la mise en action d'une structure

[87] *Éléments publics de doctrine militaire de lutte informatique défensive*, *op. cit.*, p.4.
[88] Instaurée par la *Revue Stratégique de Cyberdéfense*, *op. cit*, p.48.
[89] *Éléments publics de doctrine militaire de lutte informatique défensive*, *op. cit.*, p.4.
[90] *Ibid.* p.5.
[91] *National Cyber Strategy*, Washington, Présidence des États-Unis d'Amérique, septembre 2018, p.21 : « *All instruments of national power are available to prevent, respond to, and deter malicious cyber activity against the United States. This includes diplomatic, information, military (both kinetic and cyber), financial, intelligence, public attribution, and law enforcement capabilities* ».

située sur le territoire national, à plusieurs milliers de kilomètres.

Les armées ont également besoin d'un modèle de transition numérique à l'échelle la plus basse, à savoir le niveau tactique. Il est donc intéressant d'imaginer un modèle permettant d'analyser la manière dont les capacités numériques s'intègrent aux structures en place, tout en essayant de mesurer si cette intégration est harmonieuse ou non. Cela nécessite d'observer les mutations les plus récentes dans ce domaine relativement neuf de l'affrontement militaire, où les exemples concrets, documentés et accessibles sont, en définitive, assez rares. Nous évoquerons donc, pour conclure cette invitation au débat, la manière dont se déroule actuellement le virage numérique des forces françaises au niveau tactique.

À chaque confrontation, le rôle des outils de « guerre électronique » dans « le dernier kilomètre tactique »[92] s'avère un peu plus central. Il a d'ores et déjà permis à des groupes comme l'État Islamique ou le Front Al-Nosrah de mener des opérations *low tech* et *low budget* sophistiquées et de plus en plus difficiles et couteuses à combattre[93]. Cependant, le savoir-faire permettant de neutraliser ces moyens originaux commence à s'accumuler dans les différentes unités des armées occidentales et certaines leçons peuvent en être tirées.

Les unités de combat des trois armées françaises « traditionnelles » dépendent des nouvelles technologies de l'information et de la communication pour exécuter un nombre de tâches croissant. Si l'on retient l'hypothèse d'une numérisation toujours plus rapide des groupes belligérants et donc des conflits et des zones d'opérations tactiques, leur importance sera encore accrue demain. Elles seront par conséquent indispensables pour évoluer dans des zones hostiles de grande densité informationnelle, comme les centres urbains où pourraient avoir tendance à se concentrer les combats futurs.

Cette dépendance doit amener à une collaboration renforcée et à une meilleure cohésion entre les entités collectant le renseignement et celles l'utilisant à l'échelon tactique. Une des clés de la réussite de cette collaboration est la mise en place d'un cadre légal de collaboration efficace, permettant un travail en équipe minimisant la concurrence et le refus de collaboration (la « déconfliction » dans le vocabulaire américain), ce que nous venons d'examiner. De plus, comme le veut la logique de la numérisation que l'on peut aussi observer dans le domaine économique[94], la collaboration numérisée se doit d'être plus « horizontale » et de moins se reposer sur la circulation « verticale » des ordres et des informations utiles, tout en réservant des capacités d'intervention ciblées améliorées au profit du commandement. Un examen de la numérisation « par le bas » (l'incorporation numérique) est donc également nécessaire, après avoir examiné la transformation initiée par le sommet (la conjonction numérique).

Une première étape de l'incorporation tactique pourrait être a mise en place à tous les échelons d'officiers, de sous-officiers spécialisés dans les tâches informatiques et l'intégration de soldats-techniciens aux aptitudes moins élevées (semblables aux « opérateurs radio » présents dans chaque groupe de combat, dont la tâche a déjà évolué vers la transmission satellite et la gestion de programmes informatiques simples, notamment avec l'introduction de l'Auxylium, outil de communication numérique semblable à un smartphone). Présents en grand nombre au sein des unités les plus restreintes (en France, le groupe de combat, soit entre 8 et 12 hommes), ces nouveaux métiers de l'Armée de Terre doivent permettre une liaison

[92] Terme utilisé dans la littérature portant sur l'intégration cyber-tactique, notamment Porche, Isaac R. III & Colin, Clarke P., *Tactical Cyber*, *op. cit.*, p.26.

[93] Bronk, Chris & Anderson, Gregory, "Encounter Battle: Engaging ISIL in Cyberspace" in *Cyber Defense Review*, 2017, n° 2, vol. 1. Cf également Hashim, Ahmed S., *The Caliphate at war: Operational realities and innovations of the Islamic State*, Oxford, Oxford University Press, 2018.

[94] Voir la bonne description de cette conséquence de la numérisation sur la gouvernance des organisations de tout type dans *World Bank World Development Report 2019: The Changing Nature of Work*, Washington, International Bank for Reconstruction and Development, 2018.

numérique fiable et de pénétrer ou brouiller ceux de l'adversaire.

Le maintien une séparation stricte entre une « armée cyber » ou des unités purement dédiées à la lutte informatique mais situées à des milliers de kilomètres ne permet pas de susciter l'« esprit de corps » nécessaire à la poursuite du combat, qui reste un phénomène avant tout humain. Cette configuration ne permet pas d'établir une véritable solidarité entre les des deux équipes et aboutit souvent à l'annulation de la mission au moindre accroc par rapport au plan de départ, car la communication entre la hiérarchie et l'équipe numérique ne s'opère pas de manière optimale. L'armée américaine a ainsi mis en place depuis 2017 une hiérarchie complète d'*Electronic Warfare Officiers* et de managers du spectre électromagnétique, devant être incorporés du haut de la hiérarchie jusqu'aux derniers échelons[95].

Si l'on se place d'un point de vue opérationnel, certains enseignements peuvent d'ores et déjà être tirés de la numérisation d'unités entière et la mise en place d'un « soutien » numérique. La comparaison avec les Etats-Unis peut ici être mobilisée. Le document *Tactical Cyber : Building a Strategy for Cyber Support to Corps AMD Below*[96] est une étude portant sur l'usage d'outils « cyber-tactiques » dans trois opérations extérieures américaines, appartenant à la fois au domaine de la sécurité civile et de l'action militaire. Il s'agit en l'occurrence :

- 1) de la *joint interagency task-force-south*, traquant le trafic de drogue en provenance de l'Amérique du Sud ;
- 2) de la coopération du Corps des Marines avec la NSA pour recevoir et utiliser le Renseignement d'origine électromagnétique (SIGINT) ;
- et enfin 3) de l'utilisation des drones militaires lors de l'opération *Enduring Freedom*.

Leur point commun est de mobiliser des outils de pointe et une utilisation très précise du renseignement numérique pour la réussite de la mission. Les points les plus saillants de ces trois études de cas très fouillées peuvent être ramenés à quelques conclusions, pouvant guider la consolidation de l'échelon tactique grâce aux nouveaux outils numériques :

1) Construire une relation de coopération entre unités tactiques et services de renseignement (en particulier dans les cas où sont impliquées plusieurs agences, dont certaines appartenant à d'autres États) demande une confiance mutuelle, qui ne peut être atteinte que grâce à une collaboration prolongée. Cette coopération est bien entendu approfondie par les phases d'opérations nécessitant de nombreuses et rapides transmissions d'informations. La cohésion née de la répétition de la collaboration est précieuse et doit être mise à profit pour les opérations futures. La congruence « sodalique »[97] des groupes impliqués est primordiale pour la réussite de la mission et doit être considérée comme un problème naturel et inévitable, et son dépassement comme obstacle objectif, dont la résolution est une condition du bon déroulement des opérations.

2) La collaboration doit être bénéfique à tous les participants. Installer une compréhension mutuelle des intérêts et des principes de chaque organisme est un préalable indispensable à une saine relation de collaboration. Celle-ci peut être améliorée en échangeant des personnels et en convenant d'une procédure standard simplifiée en matière de partage d'informations. Grâce à

[95] 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, intitulé 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 ».

[96] Porche, Isaac R. III & Colin, P. Clarke, « Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below », Santa Monica, RAND Corporation, Aroyo Center, 2017.

[97] Dérivé de *sodalis/socius*, qui désigne le compagnon, l'associé, le membre d'une confrérie en latin. La sodalité doit s'entendre au sens de « capacité de former un groupe efficace pour atteindre la tâche qui lui est attribuée ». Voir Baechler, *Nature et Histoire*, *op. cit.*, p.150.

cette coopération humaine concrètement établie par le biais d'agents de liaison, les besoins de l'unité sur le terrain sont constatés par un délégué de l'agence de renseignement d'origine électromagnétique. Refuser de donner certaines informations devient alors plus difficile lorsqu'un accord humain et procédural a été établi dès le début de la coopération. Cela conduit à une identification commune aux buts de la mission et construit une communauté d'intérêts orientant les efforts dans la même direction[98].

3) Les succès de certaines opérations doivent être utilisés pour démontrer l'intérêt mutuel à la coopération et pouvoir l'approfondir (sur le modèle de la cellule Allat[99], par exemple, permettant de recouper les informations des différentes agences de renseignement françaises et ainsi déceler plus efficacement la préparation d'opérations terroristes). La démonstration de la non-hostilité doit être apportée pour établir un dialogue bénéfique à toutes les parties prenantes. On retrouve ici les fondamentaux de l'analyse des organisations bureaucratiques dans le domaine de la science politique[100].

4) Le cadre légal de l'opération doit être défini avec précision dès le départ, notamment afin que les autorisations de lancer des opérations numériques ne demandent pas une multitude de démarches au plus haut niveau et fassent manquer des opportunités tactiques au commandement. L'initiative tactique, ainsi que « l'agilité » dont parle la Revue Stratégique française de 2017, ne doivent pas être amoindries par une lourdeur procédurale privant le commandement de sa capacité d'action, dans le juste tempo du théâtre opérationnel.

C'est sur ces principes qu'a été engagée la numérisation des unités de l'Armée de Terre française, avec la mise en place du programme Scorpion. Prenant pour exemple le programme pilote « Cyber Support to Corps and Below » de l'US Army, cité par le document *Tactical Cyber* de la RAND paru en 2017[101], l'Armée de Terre cherche à doter ses troupes d'équivalents des *CyberWarfare Officers*, comme le note le lieutenant-colonel Cheize, du Centre de Doctrine et d'Enseignement du Commandement : « *[…] un chef tactique en milieu terrestre est responsable d'une zone d'opérations de plus en plus dense en termes de systèmes numériques et de volume de données, stockées et transmises par divers supports de communication, et cette tendance pourrait continuer à prendre de l'ampleur avec des moyens toujours plus performants. Il doit donc être en mesure d'agir sur cet environnement de façon réactive, soit pour défendre ses propres systèmes soumis à une menace croissante, soit pour saisir des opportunités tactiques en engageant son adversaire dans ou à travers le cyberespace* »[102].

Pour cela, la solution de techniciens dotés de compétences pouvant être multipliées dans un grand nombre de groupes tactiques semble être la meilleure. Les effets ainsi recherchés indiquent clairement un objectif centré sur le niveau tactique : « *l'enjeu pour l'armée de Terre, précise l'officier cité, est de mettre ses forces terrestres dans une position où elles seront en capacité :*

- *de fournir une appréciation de situation de leur environnement propre, par le biais d'une Situation Cyber de Référence (SCR, ou CP) ;*

[98] C'est là une constante de la collaboration militaire, comme le montre Michel Goya dans *Res Militaris : de l'emploi des forces armées au xxie siècle*, pour la collaboration entre pilotes et mécaniciens de l'USAF (Paris, Economica, 2011).

[99] Nommée d'après une déesse préislamique, cette cellule constituait un forum d'échange d'informations sur le terrorisme et le conflit irako-syrien. Ses procédures, fondées sur une sollicitation directe et une réponse immédiate de la part du service concernée, a été jugée particulièrement efficace. Ce jugement confirme que la pertinence de la stratégie du « pied dans la porte », encouragée par le rapport *Tactical Cyber*. Fondée sur la connaissance personnelle et la compréhension des besoins opérationnels des autres agences, elle a permis la circulation d'informations à un rythme bien plus rapide qu'habituellement et a mis en place une véritable « déconfliction », limitant la guerre des services et la rétention d'informations.

[100] Haas, Michael, *The Bureaucratic entrepreneur*, Washington DC, Brookings Institution Press, 2001.

[101] Porche & Clark, *Tactical Cyber, op. cit*.

[102] Cheize, Julien, « Les enjeux du cyberespace pour l'armée de Terre », in *Pensées mili-terre Centre de doctrine et d'enseignement du commandement*, publié le 21 mars 2020.

- *de défendre leurs systèmes d'armes, de commandement et de contrôle (C2), d'information ;*
- *d'identifier et demander, en appui de leur manœuvre, des effets qui seront produits par les niveaux supérieurs, jusqu'au niveau opératif ou stratégique ;*
- *de produire directement ces effets grâce à des capacités tactiques qui seraient déployées au sein d'une division, d'une BIA, voire d'un GTIA* »[103].

Ces enjeux, si on les met en parallèle du cadre conceptuel proposé dans cette note, appartiennent bien au domaine de l'i*ncorporation tactique numérique.* Bien entendu, ces nouvelles capacités ne vont pas sans de nouvelles vulnérabilités, comme le remarque Serge Caplain, de l'IFRI. Des problèmes résolus pourraient surgir des problèmes insuffisamment anticipés, liés notamment à la capacité à maintenir le lien entre les unités. Ce serait alors l'échelon tactique qui pâtirait de la somme de toutes les insuffisances accumulées en amont : « *[Les] problèmes d'interconnexion se retrouvent essentiellement aux niveaux tactiques, ceux-là même qui ont le moins de temps et de ressource pour régler les turpitudes techniques. Les conséquences les plus évidentes sont les problèmes de fidélité de transcription, de perte de vitesse dans le traitement des informations et un éventuel ralentissement de la manœuvre* »[104]. Il fait peu de doute que les problèmes de cet ordre seront l'une des principales occupations des armées ayant opéré leur intégration numérique. De leur bonne résolution dépendra le gain de puissance réel acquis grâce à la transition numérique.

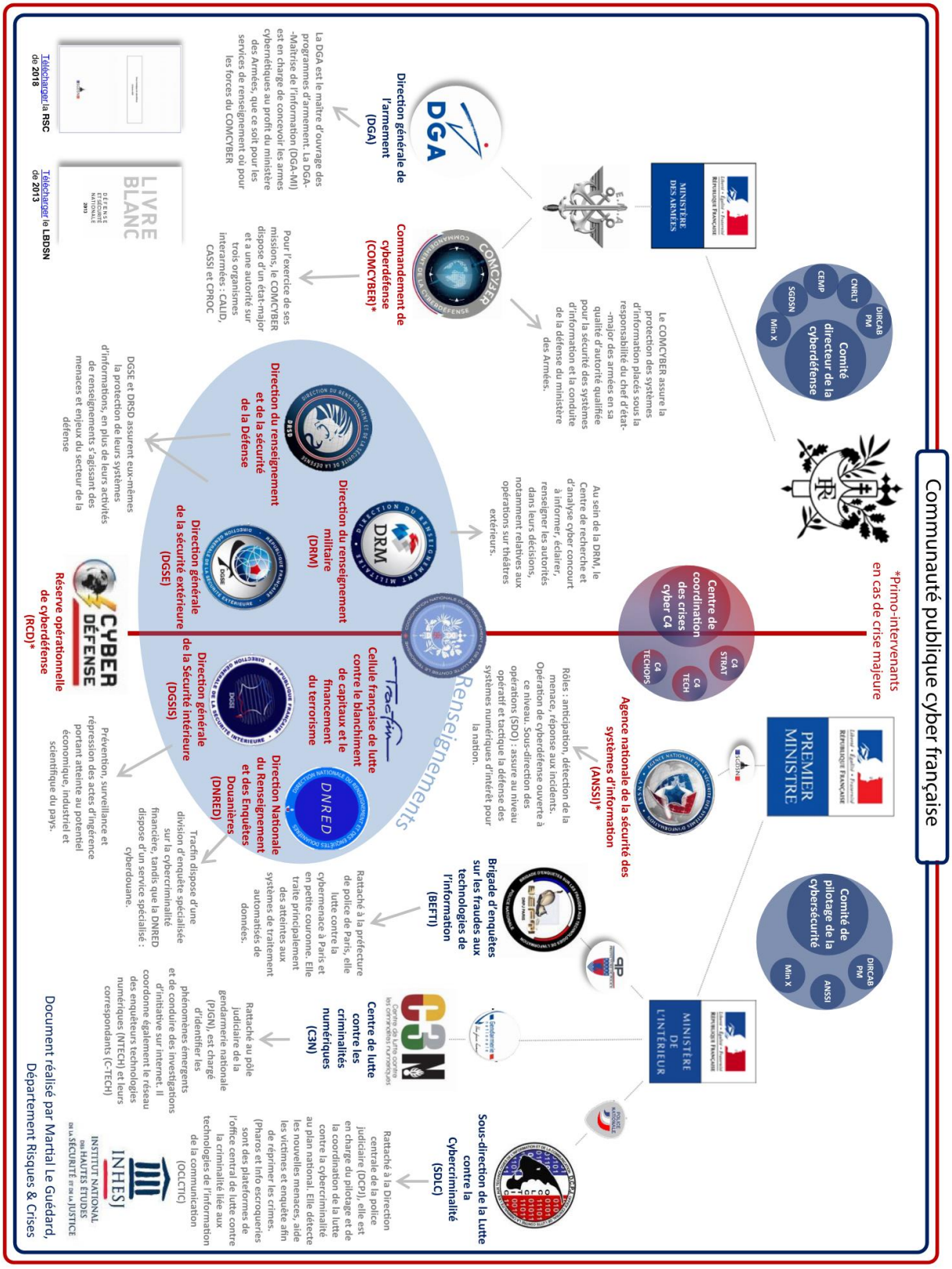
Loin d'être une pure opération technique pensée et mise en place par un ingénieur, la coopération numérique entre différentes unités elles-mêmes numérisées doit être pensée et analysée comme un processus complexe, ayant des enjeux techniques, économiques et sociaux (plus précisément sodaliques et agoriques). Ce processus, que Philippe Lépinard baptise « organisation augmentée »[105], est un enjeu en soi de la transformation numérique des armées. Comme tout phénomène humain et politique supposant un partage des ressources et du pouvoir, celui-ci met d'ores et déjà aux prises des individus et des groupes bureaucratiques aux objectifs parfois divergents, sinon antagonistes. Il s'agit donc de prendre en compte ces stratégies d'« entrepreneurs bureaucratiques », selon le terme forgé par Richard Haas[106]. Comme nous l'avons déjà souligné, ces analyses sont le résultat de l'application aux études stratégiques des outils classiques de la science politique et de la sociologie, ainsi que de l'analyse technologique ou économique.

[103] *Ibid.*

[104] Caplain, Serge, « Les 10 pièges de la numérisation des forces terrestres », article posté sur la page personnelle LinkedIn de l'auteur du 15 janvier 2018. https://www.linkedin.com/pulse/les-10-pi%C3%A8ges-de-la-num%C3%A9risation-des-forces-serge-caplain/

[105] Lépinard, Philippe, « La numérisation des forces terrestres : de la numérisation de l'espace de bataille à l'organisation augmentée », 18e Congrès de l'Association Informatique et Management, Montréal, 2018. https://hal-upec-upem.archives-ouvertes.fr/hal-01823344/document

[106] Haas, Richard, *The Bureaucratique Entrepreneur*, Washington, Brookings Institution Press, 1999.



« Communauté cyber française »,
Document réalisé par Martial Le Guédard, 2019.

En résumé, selon les éléments dégagés de l'étude *Tactical Cyber*, il semble possible de retenir quatre principes pour la mise en place d'une coopération numérique efficace : **la numérisation des armées est**

- **(1) un processus social, fondé sur une collaboration éprouvée de groupes stables…**
- **(2) ayant bâti une vision commune des objectifs à atteindre et instauré un climat de réciprocité et d'absence d'hostilité…**
- **(3) possédant par nature des stratégies bureaucratiques et des processus de prise de décision divergents…**
- **qui (4) ne doivent pas être rendus trop couteux par le cadre légal et réglementaire du commandement[107].**

Selon le principe dégagé avec brio par le géographe Pierre Gourou dans son analyse des politiques de développement (un autre type d'adaptation de systèmes techniques à un milieu moins avancé techniquement et humainement dissemblable), les procédures et les techniques d'encadrement, et même les « préjugés », doivent être considérés comme des « obstacles objectifs »[108] à l'implantation de nouvelles techniques. Perçues comme des « progrès » chez les humanitaires, elles peuvent cependant apparaître comme une régression sociale et économique aux personnes que l'on cherche à aider. Tout comme les politiques de développement, la transition numérique doit prendre comme « obstacle objectif » la configuration cognitive des soldats, qui doivent s'acquitter de tâches complexes pour lesquelles la stabilité est un gage de sûreté.

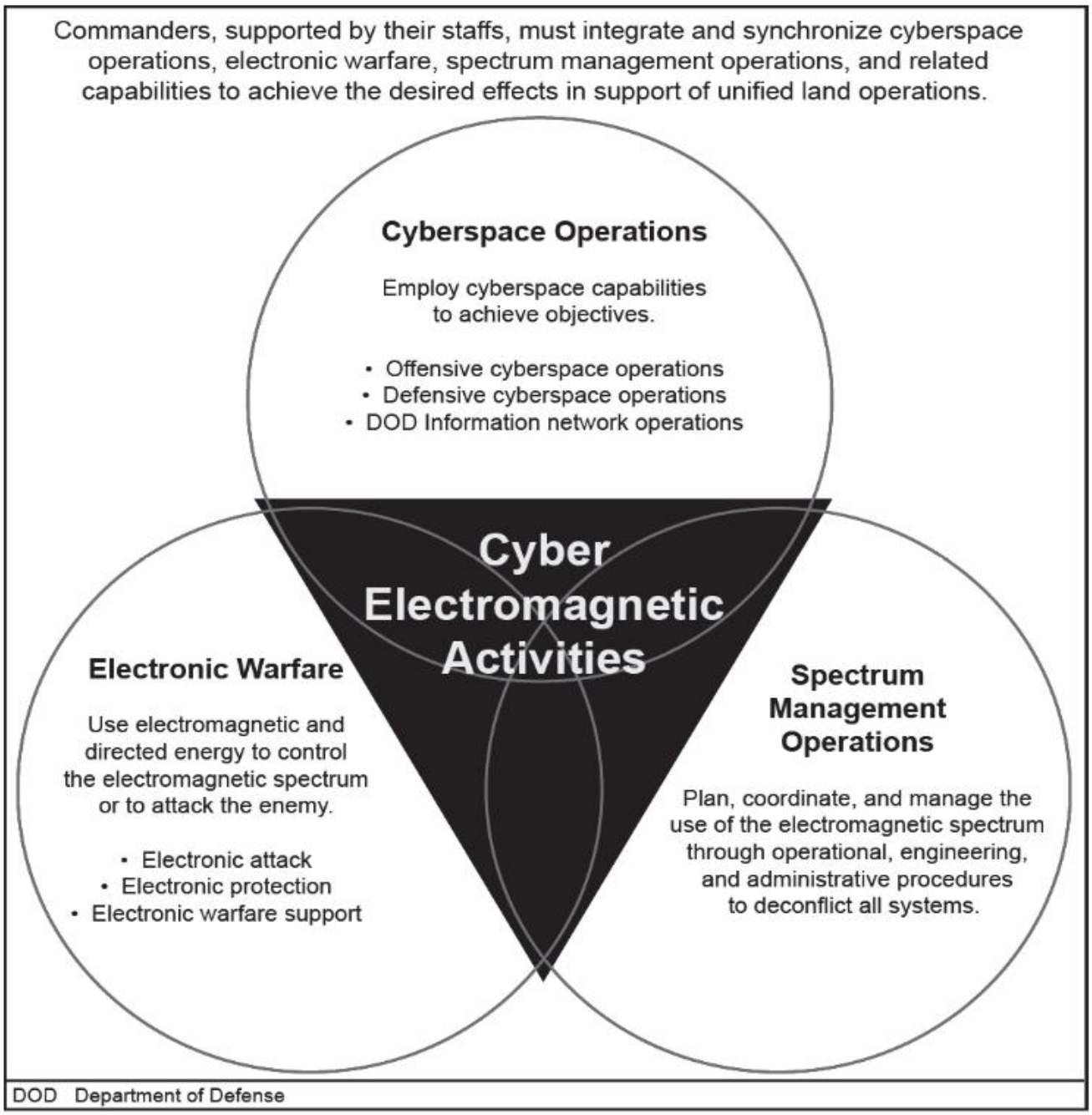
Une transition numérique bientôt achevée ? L'exemple de l'*Advanced Battle Management System* de l'US Air Force

Cet objectif d'adaptation aux facultés cognitives des soldats est décelable dans l'un des projets les plus pointus actuellement menés par le Département de la Défense américain : l'*Advanced Battle Management System* (ABMS). Il s'agit ici du nouveau modèle de Command & Control de l'US Air Force, basé sur une architecture de données totalement refondue pour faire face aux flux d'information encore impossibles à traiter, car générés par les très nombreux capteurs mis en place par le Pentagone sans que le nombre d'analystes équivalent soit ouverts. C'est, à bien des égards, une nouvelle génération de « système de commandement et de coordination » qui pourrait créer un précédent et fournir le premier modèle d'une armée dont l'ensemble des éléments seraient intégrés à un canevas numérique pensé à l'échelle d'une armée entière.

Ce concept de « Système de Gestion Avancée du Combat » est la déclinaison de la doctrine des Opérations Multi-Domaine (rebaptisée *Joint All Domain Operations* par l'armée de l'air américaine) en termes de *Command & Control* numérisé. L'objectif est ici de « *[…] créer des dilemmes pour les forces adverses, surpassant leurs capacités avec une quantité trop importante de menaces à contrer de manière efficace* »[109], en faisant bénéficier l'ensemble des « effecteurs » des données recueillies par les capteurs beaucoup plus avancés dont bénéficient les appareils de dernière génération, comme le F-35. En effet, ainsi que le souligne le Lieutenant General David S. Nahom, Chef d'Etat-Major adjoint de l'US Air Force responsable de la Planification, l'infrastructure de données actuelle est insuffisante pour tirer pleinement partie des possibilités offertes par ces aéronefs : « *[…] le F-35, juge-t-il ainsi, produit des données d'un volume dont n'était capable aucun avion auparavant. Comment partageons-nous cette information avec une équipe de forces*

[107] Porche & Clark, *Tactical Cyber*, *op. cit.*
[108] Gourou, Pierre, *Les Terres de Bonne Esperance : le monde tropical*, Paris, Plon, coll. « Terre Humaine », 1982, p.284.
[109] *Ibid., p.4.*

spéciales précise se trouvant au sol ? Nous devons construire une infrastructure qui permette cela »[110]. C'est donc la mise en réseau des capteurs *et* des effecteurs de l'ensemble des forces armées qui est nécessaire. « *Armée de l'Air, Marine, Armée de Terre, Corps des* Marines*, nous avons tous des capteurs déployés. La question est comment nous nous plaçons tous au sein d'une même boucle, pour que nous puissions partager des informations d'une qualité suffisante pour pouvoir ouvrir le feu* »[111].



[110] Entretien du Lt General David S. Nahom, USAF Deputy Chief of Staff for Plans and Programs, pour le Mitchell Institute for Aerospace Studies, 16 avril 2020, https://www.youtube.com/watch?v=VPWsdbr3BZc. "*Those F-35 are bringing in data information at a level no other airplane on earth has ever been able to do. How do we get to a point where we can share this information with that special ops team directly below that airplane? We need to build an infrastructure that allows that*".

[111] *Ibid.*, "*Air Force, Navy, Marines, Army… everyone has a sensor out there. The question is how do we loop them all in, so we can share data at shot quality level*".

La mise en place d'une nouvelle architecture de données est donc une manière d'améliorer drastiquement la vitesse d'acquisition des cibles pour mener des attaques « tous azimuts ». Elle pourrait également se révéler une nécessité pour permettre au système de fonctionner convenablement, sans crouler sous le poids exponentiel de la donnée recueillie. Comme le précise la demande de budget de l'US Air Force pour l'année fiscale 2021[112], l'ABMS est tout autant perçu comme une évolution nécessaire des capacités offensives qu'une mise à jour vitale du circuit informationnel. Celui-ci est en effet placé, à l'heure du retour des « *near-pear adversaries* », sous la double menace de sa propre complexité et des nouvelles performances dont sont capables les opposants potentiels, notamment grâce à la diffusion des technologies numériques à bas coût : « *La connexion de ces plateformes, capteurs et armes via ABMS et le* Joint All-Domain Command AMD Control *maintiendra leur viabilité et la létalité au combat* »[113].

Cependant, le succès de cette réforme pourrait donner à l'US Air Force une supériorité tactique et stratégique lui permettant de maintenir, voire même de renforcer la *Total Air Dominance* dont elle bénéficie encore à l'heure actuelle. Grâce à l'apport de technologies numériques et du traitement automatique de certaines tâches par l'intelligence artificielle, l'état-major de l'armée de l'air américaine espère ainsi « *générer une fenêtre de supériorité dans les airs et dans le cyberespace, les forces interarmées (*joint*) convergeant vers les cibles les plus importantes* »[114].

L'idée d'une *Total Cyber Dominance* ou d'une *Cyber-Supremacy* qu'il sera nécessaire d'établir, parallèlement à la suprématie aérienne[115], affleure dans cette demande de budget rendant explicite les objectifs ultimes du système de combat à venir de l'Amérique. De plus, la gestion de l'information étant facilitée, des bénéfices concrets s'offriraient au personnel opérationnel. Par exemple, l'activité des pilotes pourrait être recentrée sur le combat, et s'éloigner de la communication permanente avec les escadrons et le C2 : « *Un essai récent a consisté à connecter les ordinateurs de deux avions furtifs de l'Air Force – un F-22 Raptor et un F-35 Joint Strike Fighter – ce qui leur a permis de partager des données automatiquement, afin que leurs pilotes puissent passer moins de temps à se parler et plus de temps à évaluer les données et agir sur elle* »[116]. Une augmentation de la capacité de destruction et d'évitement des menaces est également attendue de cette numérisation du *Command & Control*, qui constitue un pas important dans l'amélioration *conjonction stratégique*.

Les quatre armées américaines seraient ainsi en mesure de transmettre données et positions, qu'elles concernent aussi bien l'ennemi qu'elles-mêmes, à tout moment et de manière automatique. « Lorsque l'Air Force emploiera de concert les capacités de l'Armée, de la Marine, du Corps des Marines et de la Force spatiale, les adversaires devront défendre leurs forces dans tous les domaines, à tout moment. L'Air Force rendra possible les *Joint All-Domain Operations* en aidant à connecter toutes les forces dans un réseau de combat cohérent d'une manière qu'elles ne possèdent pas aujourd'hui »[117].

Quelques interconnexions pourront ainsi être envisagées afin de réaliser la tâche la plus ardue actuellement : l'acquisition de cible partagée et automatisée, non pas entre plusieurs armes, mais plusieurs armées, voire avec des forces alliées : « Par exemple, précise l'US Air Force dans sa demande de budget 2021 au Congrès américain,

---

[112] *United States Air Force Posture Statement Fiscal Year 2021*, Washington, *Department of Defense*, février 2020.
[113] *Ibid., p.5.*
[114] *Ibid.*
[115] Sur l'idée de supériorité informationnelle, voir Wielhouwer, Peter W., « Toward Information Supériority: The contribution of Operational Net Assessment », in *Air & Space Power Journal*, Vol. XIX, n° 3, pp.85-96. Pareillement, ce concept est sous-jacent dans le titre même du programme dit de « *Next Generation Air Dominance* », souvent abrégé en NGAD, concevant la 6e génération d'avion de combat de l'US Air Force.
[116] Tucker, Patrick, "Toward A War With Fewer Radio Calls." In *Defense One*, 21 janvier 2020, https://www.defenseone.com/technology/2020/01/toward-war-fewer-phone-calls/162562/
[117] *United States Air Force Posture Statement Fiscal Year 2021*, *op. cit.*, p.2.

nos avions de cinquième génération ne peuvent pas facilement partager des données avec certains chasseurs plus anciens, les capteurs de nombreux navires de la Marine ne peuvent pas détecter les batteries de l'artillerie de défense aérienne de l'Armée de Terre et les soldats et les *Marines* ne peuvent pas toujours accéder aux flux vidéo en temps réel de nos partenaires internationaux durant le combat ».[118]

La caractéristique majeure de ce système est ainsi la capacité à fournir une architecture numérique permettant une circulation de données simple, où l'ensemble des partenaires peuvent « se brancher » sans trop de difficulté, tout en permettant une maîtrise des données partagées. Mais pour réussir, la mise en place de cette nouvelle architecture doit être massive et englober l'ensemble des effecteurs disponibles, tout en posant une nouvelle norme pour les futures acquisitions. Effectuée sans cohérence, la numérisation connaîtrait une somme cumulée de retards et de sous-performances qui rendraient impossible tout gain de puissance réel : « *L'Air Force considère l'architecture ABMS comme la clé pour éviter de créer un effort d'acquisition massif à partir de programmes disparates comme Reaper ou la flotte JSTARS héritée* »[119]. L'idée sous-jacente est ici que cette transition numérique globale pourrait même n'être possible que dans une fenêtre temporelle restreinte, avant que ne viennent s'agréger une quantité trop importante de systèmes automatisés et de données d'origine spatiale.

En effet, si ces nouveaux moyens venaient à être « branchés » grâce à des normes propres, cela retarderait sans nul doute la capacité à partager et recevoir des informations en continu. À plein rendement, le système ABSM « *comprendra un mélange d'avions habités traditionnels, de drones, de technologies spatiales et de liaisons de données* »[120]. Or « *il est très facile de commencer à parler des satellites et des avions et d'oublier ce dans quoi l'ABMS va devoir principalement exceller, qui est l'architecture de données qui les reliera* », explique Will Roper[121], directeur du département acquisition de l'US Air Force. Une fois cette architecture de donnée sécurisée et rendue performante avec l'ensemble des aéronefs, serait activée « *la mise en réseau* ad hoc*, qui permettra aux plates-formes de commencer automatiquement à travailler ensemble et à partager des informations sans ingérence humaine* »[122].

Si l'on se fonde sur les projections techno-optimistes de la grande majorité des architectes de force américains, c'est donc seulement une fois le cycle complet de la numérisation achevé que les capacités numériques seront en mesure d'apporter un appui aux forces « cinétiques » bien plus probant grâce aux nouvelles configurations permises par l'ABMS. Selon le général James Holmes, qui dirige le *Air Combat Command*, ce n'est qu'à ce moment-là que la contribution les nouveaux moyens numériques participeront pleinement à la prise de décision stratégique : « *Nous pensons que nous pouvons présenter des équipes plus robustes [au Cyber Command] avec un meilleur support de renseignement derrière elles et ainsi présenter des options et des informations opérationnelles […] à une bien plus grande échelle* »[123].

Si ces promesses sont tenues, le système ABMS pourrait être étendu à l'ensemble des forces armées américaines. Le budget demandé par le Pentagone pour 2021 y consacre 302 millions de dollars, contre 144 millions de dollars votés pour 2020[124]. On constate donc une véritable montée en puissance de cette architecture numérique qui

---

[118] *Ibid.*

[119] Insinna, Valérie,, « Here's the Number One rule for Air Forces New Advanced Battle Management System », in *Defense News,* 9 juillet 2019. https://www.defensenews.com/digital-show-dailies/paris-air-show/2019/07/09/rule-no1-for-air-forces-new-advanced-battle-management-system-we-dont-start-talking-platforms-until-the-end/

[120] *Ibid.*

[121] *Ibid.*

[122] *Ibid.*

[123] Pomerleau, Mark,. "How A New Air Force Unit Could Help Beat Russian Air Defense Systems", in *C4ISRNET*. 12 novembre 2019, https://www.c4isrnet.com/battlefield-tech/it-networks/2019/11/12/how-a-new-air-force-unit-could-help-beat-russian-air-defense-systems/

[124] *United States Air Force Posture Statement Fiscal Year 2021*, *op. cit.*, p.2.

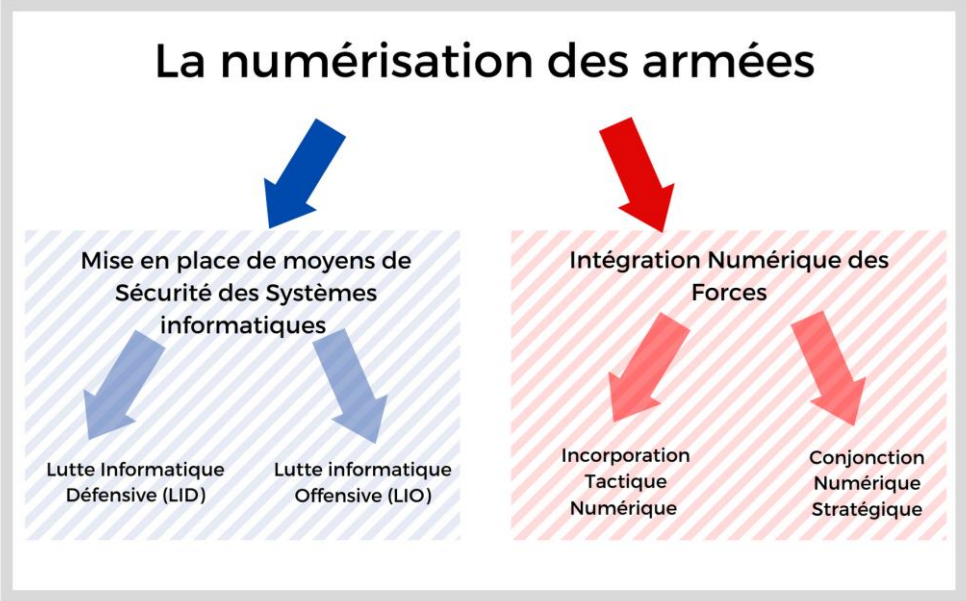


Fig.2 Les étapes de la numérisation des armées
Antony Dabila, 2020.

pourrait voir son enveloppe budgétaire doubler l'année prochaine. En effet, « *l'ABMS fait partie d'une vision plus large du Pentagone appelée* Joint All-Domain Command & Control. *Le JADC2 représente un effort pour créer un système nerveux en réseau pensé pour la guerre. Il vise à relier tous les navires, tous les soldats et tous les avions à réaction, de sorte que les ressources terrestres, aériennes, maritimes, spatiales et cybernétiques puissent partager exactement les mêmes données, qui pourront être utilisées de manière presque interchangeable pour éliminer des cibles, même dans des environnements où la communication est fortement sollicitée, brouillée, ou là les adversaires ont des défenses aériennes avancées* »[125]. L'armée américaine serait alors la première armée à avoir totalement achevé sa transition numérique, en conciliant les deux « pans » de l'intégration numérique optimisée proposés dans cette note : d'une part *l'incorporation* tactique, d'autre part la *conjonction* stratégique.

Conclusion : cyberespace de bataille ou nouveaux outils de commandement et de communication numériques ?

La numérisation des armées pose, comme nous avons essayé de le montrer de manière très synthétique, une série de défis humains, organisationnels et « sodaliques » qu'il serait dommageable de négliger. Les problèmes qu'elle pose aux états-majors apparaissent autant liés à l'émergence de nouveaux outils techniques qu'à leur manipulation par des groupes de combat aux habitudes éprouvées et coûteuse à modifier. Les outils d'interprétation issus de l'anthropologie nous permettent d'évaluer, sous certains aspects, la rationalité forcément limitée des acteurs, et de combler le gouffre entre l'optimum technique imaginé *in abstracto* et les usages émergents concrètement observés. Les concepteurs des armées futures pourront difficilement se passer de ces outils d'in-

[125] Patrick Tucker, "War On Autopilot? It Will Be Harder Than The Pentagon Thinks." in *Defense One*, 12 février 2020.

terprétation, s'ils désirent véritablement établir un diagnostic et mettre en œuvre des rectifications concrètes pour accomplir la tâche qui leur incombe : implanter les outils de communication et de production de données informatiques au sein des armées « cinétiques » au moindre coût économique, humain et « cognitif » pour obtenir le maximum de puissance face aux adversaires étatiques et infra-étatiques auxquels les troupes seront confrontées demain.

Pour cela, un savoir-faire opérationnel entièrement nouveau doit, de fait, être constitué et instiller dans la formation des officiers de l'ensemble des armées. Sa qualité dépend de la pertinence de la réponse à deux problématiques : celle de l'intégration de la composante numérique à la prise de décision stratégique et tactique, et celle de la circulation rapide des innovations pouvant permettre de disposer d'un avantage ponctuel.

Pour cela, il n'est nul de besoin de fonder une armée distincte, ni de faire du cyber un espace géographique à part entière. Ne pas considérer que l'outil numérique est le « 4e domaine » de la guerre n'aboutit en rien à le déconsidérer ou en minorer le rôle. Bien au contraire, il s'agit d'insister sur la transversalité totale du système technique numérique et le placer au centre de toutes les opérations relevant du ministère des Armées (fig. n° 1). C'est aussi considérer que sa place est centrale dans la prise de décision et qu'une bonne intégration organisationnelle est le gage d'une meilleure agilité tactique et d'une capacité d'improvisation et d'adaptation aux situations imprévues renforcées. Plutôt que la mise en place organique d'armées dédiées au « cyber », Il est vraisemblablement plus constructif d'opter pour des forces armées entièrement intégrées numériquement, c'est-à-dire cyber-transversalisées.

Ce débat est crucial pour les armées de l'Alliance atlantique en particulier, qui pourraient voir leur prééminence remise en cause si de mauvais choix en termes de politique de numérisation étaient effectués. Les décisions prises aujourd'hui engagent les armées françaises dans une *path dependence* qui pourrait amoindrir durablement leur capacité d'action, déjà entamée par la multiplication des crises, des interventions extérieures et par la diffusion des outils numériques eux-mêmes, qui ont facilité le potentiel de nuisance opérationnelle de groupes autrefois dépourvus de toute influence réelle sur les relations internationales.

Les conséquences, nécessairement imprévisibles, de la transformation technique et sociale liée à la numérisation des opérations doivent être scrutées étape par étape, afin de comprendre la nature des changements humains que l'on est en train de provoquer. « *Chaque situation locale étant un complexe de techniques qui réagissent les unes sur les autres* »[126], selon P. Gourou, l'analyse de la *transition numérique des armées* ne peut faire l'impasse sur une enquête anthropologique pluridisciplinaire permettant d'évaluer au fur et à mesure les conséquences humaines du changement technique sur la microsociologie du groupe social auquel on l'impose. *À fortiori* si ce groupe n'est pas un régiment de « cyber-combattants » monté de toute pièce et évoluant en vase clos au sein de l'armée, mais des groupes de guerriers traditionnels auxquels on accole de nouveaux ensembles techniques numériques.

Ainsi pourrait émerger la possibilité d'un outil d'analyse non pas seulement technique, mais également humain, qui permettrait sans doute d'orienter de manière plus fine les choix politiques et stratégiques qui doivent être faits aujourd'hui et qui auront, dans la décennie à venir, les répercussions les plus décisives sur le rapport de forces entre les différentes puissances de la scène internationale.

[126] Gourou, Pierre, *Les Terres de Bonne Esperance : le monde tropical, Paris, Plon, coll. « Terre Humaine », 1982*, p.370.

Bibliographie

Ouvrages

ANDRESS, Jason & WINTERFELD, Steve, *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners*, Amsterdam, Syngress, 2011

BARNABY, Frank, *The Automated Battlefield: New technologies in modern warfare,* Oxford, Oxford University Press, 1986.

BARNABY, Frank, *What on Earth is Star Wars?: Guide to the Strategic Defence Initiative*, Fourth Estate Ltd, 1987.

BAECHLER, Jean, *Nature et Histoire*, Paris, PUF, 2000.

BONNEMAISON, Aymeric & DOSSE, Stéphane, *Attention : Cyber ! Vers le combat cyber-électronique*, Paris, Economica, 2014.

BOYER, Bertrand, *Cyberstratégie, l'art numérique de la guerre*, Paris, Nuvis, 2012.

BOYER, Bertrand, *Cybertactique, conduire la guerre numérique*, Paris, Nuvis, 2014.

BUCHANAN, Ben, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Oxford, Oxford University Press, 2017.

CARR, Jeffrey, *Inside Cyberwarfare*, Sebastopol (California), O'Reilly, 2009.

CLAUSEWITZ, Carl von, *De la Guerre*, Paris, Editions de Minuit, 1955.

COUTAU-BEGARIE, Hervé, *Traité de Stratégie*, Paris, Economica, 2011 (7e édition).

DABILA, Antony, *L'Engagement militaire : essai de sociologie comparée*, thèse soutenue à l'Université Paris-Sorbonne le 5 novembre 2013 https://www.theses.fr/2013PA040132.pdf

DEPTULA, David & PENNEY Heather, *Restoring America's Military Competitivness : Mosaic Warfare*, Arlington (Virginie), The Mitchell Institute for Aerospace Studies, septembre 2019.

GIBSON, William, *The Neuromancer,* New York, Ace Books, 1984.

GOUROU, Pierre, *Les Terres de Bonne Espérance : le monde tropical*, Paris, Plon, coll. "Terre Humaine", 1982.

GOYA, Michel, *Res Militaris : de l'emploi des forces armées au XXIe siècle*, Paris, Economica, 2011.

HAAS, Richard, *The Bureaucratic Entrepreneur*, Washington, Brookings Institution Press, 1999

HASHIM, Ahmed S., *The Caliphate at war : Operational realities and innovations of the Islamic State*, Oxford, Oxford University Press, 2018.

HENROTIN, Joseph, *Techno-guérilla et guerre hybride*, Paris, Nuvis, 2014.

HUYGHE, François-Bernard, KEMPF, Olivier & MAZZUCHI, Nicolas, *Gagner les cyberconflits*, Paris, Economica, 2015.

KAPLAN, Fred, *Dark Territory: The Secret History of Cyber War*, New York, Simon & Schuster, 2016.

KEMPF, Olivier, *Introduction à la cyberstratégie,* Paris, Economica, 2012.

KEMPF, Olivier, *Alliances et mésalliances dans le cyberespace,* Paris, Economica, 2014.

KEMPF, Olivier, DOSSE, Stéphane & MALIS, Christian, *Le Cyberespace, nouveau domaine de la pensée stratégique,* Paris, Economica, 2014.

LIA, Brynjar, *Architect of global Jihad*, London & New York, Hurst &Columbia University Press, 2008

RID, Thomas, *Cyberwar will not take place*, Londres, Hurst, 2017 (2e ed.).

RID, Thomas, *Rise of the Machines: A Cybernetic History*, Londres, Norton & Cie, 2017 (2e ed.).

SIMONDON, Gilbert, *Du Mode d'existence des objets techniques*, Paris, Aubier-Montaigne, 1958.

SINGER, Peter W. & FRIEDMAN, Allan, *Cybersecurity & Cyberwar : What everyone needs to know*, Oxford, Oxford University Press, 2014

VENTRE, Daniel, *La Guerre de l'Information*, Paris, Hermès Lavoisier, 2007.

VENTRE, Daniel, *Cyberguerre et guerre de l'information : stratégies, règles et enjeux*, Paris, Hermès Lavoisier, 2010.

VENTRE, Daniel, *Cyberespace et acteurs du cyberconflit*, Paris, Hermès Lavoisier, 2011.

VENTRE, Daniel, *Cyberattaque et Cyberdéfense*, Paris, Hermès Lavoisier, 2011.

VENTRE, Daniel, *Chinese Cybersecurity and Defense*, Londres, Wiley-ISTE, 2014.

VENTRE, Daniel, *Information Warfare*, Londres, Wiley ISTE, 2016.

WIENER, Norbert, *Cybernetics, or control and communication in the animal and the machine*, Cambridge, Massachusetts, MIT Press, 1948 (trad. fr. *La Cybernétique, information et regulation dans le vivant et la machine,* Seuil, 2014).

WIENER, Norbert, *Cybernétique et Société*, Paris, Seuil, 2014 (1er ed. américaine 1950)

Articles

ALLEN, Greg & CHAN, Daniel, « Artificial Intelligence and National Security », Belfer Center for Science and International Affairs, Cambridge, Massachusetts, juillet 2017.

ARQUILLA, John & RONFELD David, *Cyberwar is coming!*, Santa Monica, RAND Corporation, 1993.

ARQUILLA, John, « Cyberwar Is Already Upon Us » in *Foreign Policy*, 27 février 2012.

BALZACQ, Thierry & DUNN CAVELTY Myriam, « A theory of actor-network for cyber-security » in *European Journal of International Security*, Vol.1, n° 2, Juillet 2016, pp.176-198.

BAUD, Michel, « La cyberguerre n'aura pas lieu, mais il faut s'y préparer », in *Politique étrangère* 2012, n° 2 (Eté), pp.305-316.

BERTHIER, Thierry & KEMPF, Olivier, « Vers une géopolitique de la donnée », in *Annales des Mines — Réalités industrielles*, 2016, n° 3, pp.13-18.

BOEHM, Barry, « A Spiral Model of Software Development and Enhancement », in *ACM SIGSOFT Software Engineering Notes*, ACM, n° 11, vol.4, pp.14-24, août 1986.

BOTT, Jonathan, « What's After Joint? Multi-Domain Operations as the Next Evolution in Warfare », United States Air Force School of Advanced Military Studies, Fort Leavenworth, 2017.

BRONK, Chris & ANDERSON, Gregory, « Encounter Battle: Engaging ISIL in Cyberspace » in *Cyber Defense Review*, 2017, n° 2, vol. 1.

CEBROWSKI, Arthur, « Transforming Transformation: Will it Change the Character of War? » in *Transformation Trends*, Département de la Défense, Office of Force Transformation, États-Unis, 2004.

CHEIZE, Julien, "Les Enjeux du cyberespace pour l'Armée de Terre", *Cahiers de la pensée Mili-Terre*, Centre de Doctrine et d'Enseignement du Commandement, 21 mars 2020.

DEPTULA, David & PENNY, Ether & GUNTZINGER, Mark, « Restoring Americas's Military Competitivness: Mosaic Warfare », Arlington (Virginie), The Mitchell Institute for Aerospace Studies, septembre 2019.

DUCHEINE, Paul, « Cyber warfare is taking place! » in *Internationale Spectator*, 2016, n° 6.

GARTZKE, Erik, « The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth » in *International Security*, vol. 38, N° 2, automne 2013, pp.41–73.

GARTZKE, Erik & LINDSAY, John, « Coercion through Cyberspace: The Stability-Instability Paradox Revisited » in Kelly M. Greenhill and Peter J. P. Krause (ed), *The Power to Hurt: Coercion in Theory and in Practice*, Oxford, Oxford University Presse, 2018.

GOURE, Daniel, « The M1-A2 Abrams is the tank of the future », *The National Interest*, 3 novembre 2018.

IASIELLO, Emilio, « Are Cyber Weapons Effective Military Tools? » in *Military & Strategic Affairs,* vol.7, n° 1, march 2015.

INSINNA, Valerie, « Here's the number one rule for Air Forces new advanced management System », *Defense News*, 9 juillet 2019.

KASPERSKY, Eugène, « Cyberguerre : « Il n'y a aucune preuve » selon Eugène Kaspersky », *Usbek et Rica,* 29 juin 2019, Consulté le 10 juillet 2019, https://usbeketrica.com/article/cyberguerre-il-n-y-a-aucune-preuve?fbclid=IwAR1PZybPmU6qyr520VafxmbC3SSXL0qxPOEIOhEP-uh9UeUGooIKtIfqohk

KURTI, Erdelina & HAFTOR Darek, « The Role of Path Dependence in the business model adaptation: from traditional to digital models », Proceedings of the 2014 Mediterranean Conference on Information Systems, Paper 28.

LAGNEAU, Laurent, « Nexter prépare une version du char Leclerc capable de mettre en œuvre des drones aériens », *Zone Militaire*, 21 février 2019

LAWSON, Sean, « Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States » in *First Monday*, Vol.17, n° 7, juillet 2012.

LEPINARD, Philippe, « La numérisation des forces terrestres : de la numérisation de l'espace de bataille à l'organisation augmentée », 18e Congrès de l'Association Informatique et Management, Montréal, 2018.

LOCATELLI, Andrea, « The Offensive/Defensive balance in Cyberspace » in *Analysis,* n° 203, octobre 2013.

LYNN, William J. III, « Defending a New Domain: The Pentagon's Cyberstrategy » in *Foreign Affairs*, September/October 2010.

MURAWIEC, Laurent, « La Cyberguerre », in *Agir, Revue Générale de Stratégie*, décembre 1999, n° 2.

NAKASONE, Paul M., « Interview with general Nakasone », *Joint Forces Quarterly,* n° 92, 1er trimester 2019, pp.4-9

NAHOM, David, « Interview with gen. David Nahom", Mitchell Institute for Aerospace Studies, 16 avril 2020.

PAUL, Philippe, « Notions sur le combat collaboratif et observation récente des expérimentations », Cahiers de la pensée mili-terre, Paris, Centre de Doctrine et d'Enseignement du Commandement, juin 2019.

POMERLEAU, Mark, « How A New Air Force Unit Could Help Beat Russian Air Defense Systems », in *C4ISRNET*. 12 novembre 2019, https://www.c4isrnet.com/battlefield-tech/it-networks/2019/11/12/how-a-new-air-force-unit-could-help-beat-russian-air-defense-systems/

PORCHE, Isaac R. III & COLIN, P. Clarke, « Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below », Santa Monica, RAND Corporation, Aroyo Center, 2017.

POST, Jonathan, « Cybernetic War », in *Omni*, mai 1979.

SINGEL, Ryan, « White House Cyber Czar : There is no Cyberwar » in *Wired,* 3 avril 2010.

SINGER, Peter & SHACHTMAN, Noah, « The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive », *Brookings*, 15 août 2011.

SUTTON, Walter S., « Cyber Operations and the Warfighting Functions », *United States Army War College*, Carlisle, Pennsylvania, 2013.

STEEL, Cherie & STEIN Arthur A., "Communications Revolutions and International Relations", in Juliann Emmons Allison (dir.), *Technology Development and Democracy: International conflict and Cooperation in the Information Age*, Albany State University of New York Press, 2002, pp.25-53.

TUCKER, Patrick, « Toward a War with fewer radio calls », *Defense One*, 21 janvier 2020.

TUCKER, Patrick, « War on auto-pilot? It will be harder than the Pentagon thinks », *Defense One,* 12 février 2020.

VENTRE, Daniel, « Cyberguerre » in *Dictionnaire de la Paix et de la Guerre*, Paris, PUF, 2017.

WIELHOUVER, Peter W. « Toward Information Supériority: The contribution of Operational Net Assessment », in *Air & Space Power Journal*, Vol. XIX, n° 3, pp.85-96.

Documents officiels

États-Unis

« Guide for Cyber Operations », *United States Department of Defense,* 2006.

« Joint Terminology for Cyberspace Operations », *United States Department of Defense,* 2010.

« Cyberspace Operations Concept Capability Plan 2016-2028 », TRADOC Pamphlet 525-7-8, *United States Department of Defense*, 22 février 2010.

« ADP 6-0 : Mission command », Joint Publications, *United States Department of Defense*, mai 2012.

« ADRP 6-0 : Mission command », Joint Publications, *United States Department of Defense*, mai 2012.

« Cyberspace Operations », Joint Publications, *United States Department of Defense*, 5 février 2013.

« Field Manual 3-12 (R) – Cyberspace Operations », Joint Publications, *United States Department of Defense*, 5 février 2013.

« Field Manual 6-0 — Commander and Staff Organization and Operations », Joint Publications, *United States Department of Defense*, mai 2014.

« Field Manual 3-12 – Cyberspace and Electronic Warfare Operations », Joint Publications, *United States Department of Defense*, 5 février 2013.

« ATP 6-02.70 – Techniques for Spectrum Management Operations », Joint Publications, *United States Department of Defense*, décembre 2015.

« ADRP 3-0 : Operations », Joint Publications, *United States Department of Defense*, novembre 2016.

« Strategic Cyberspace Operations Guide », *United States Army War College*, Carlisle, Pennsylvania, juin 2016.

« Securing Cyber Assets: Adressing Urgent Cyber Threats to Critical Infrastructure », *National Infrastructure Advisory Council*, Washington, août 2017.

« National Cyber Strategy », Washington, Présidence des États-Unis d'Amérique, septembre 2018.

« National Defense Authorization Act (NDAA) for Fiscal Year 2019 », Public Law n° 115-232

« Us Space Force Facts Sheet », 19 décembre 2019, Washington, Departement of Defense, https://www.spaceforce.mil/About-Us/Fact-Sheet.

« United States Air Force Posture Statement Fiscal Year 2021 », Washington, Department of Defense, février 2020.

France

« Livre Blanc de la Défense et de la Sécurité Nationale », *Ministère de la Défense*, Paris, 2008.

« PP30, plan prospectif à 30 ans », *Ministère de la Défense*, Paris, 2009.

« Rapport sur la cyberdéfense », Jean-Marie Bockel, Sénat de la République Française, juillet 2012.

« Rapport sur le risque numérique : en prendre conscience pour mieux le maîtriser », Bruno Sido & Jean-Yves Le Déaut, Assemblée Nationale et Sénat de la République Française, 3 juillet 2013.

« Livre Blanc de la Défense et de la Sécurité Nationale », *Ministère de la Défense*, Paris, 2013.

« Guide d'Hygiène Informatique », *Agence Nationale de Sécurité des systèmes informatiques*, Paris, 2014.

« Strategie Nationale de Securite Numerique », *Secrétariat Général de la Défense et de la Sécurité Nationale*, Paris, 2015.

« L'emploi des forces terrestres dans les opérations interarmées » (DFT 3.2 Tome 1 [FT-03]), Paris, Ministère de la Défense, 1er juillet 2015

« Rapport sur la présence et l'emploi des forces armées sur le territoire national », Olivier Audibert-Trouin & Christophe Léonard, Assemblée Nationale et Sénat de la République Française, 22 juin 2016

« L'armée de Terre Au Contact », *Terre Information Magazine*, Ministère de la Défense, Paris, juillet-aout 2016.

« Guide d'Hygiène Informatique », *Agence Nationale de Sécurité des systèmes informatiques*, Paris, 2017.

« Chocs Futurs : Étude prospective à l'horizon 2030 : impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité », *Secrétariat Général de la Défense et de la Sécurité Nationale*, Paris, avril 2017.

« Projet de loi de finance 2018 "Défense" », Assemblée Nationale de la République Française, septembre 2017.

« Revue Stratégique », *Secrétaire Général de la Défense et de la Sécurité Nationale*, Paris, 1 octobre 2017

« Revue Stratégique de Cyberdéfense », Paris, *Secrétaire Général de la Défense et de la Sécurité Nationale*, 12 février 2018

« Rapport sur les enjeux de la numérisation des armées », Olivier Becht & Thomas Gassilloud, Assemblée Nationale et Sénat de la République Française, 30 mai 2018.

« Politique ministérielle de lutte informatique défensive », Paris, *Ministère des Armées,* janvier 2019.

« Politique ministérielle de lutte informatique offensive », Paris, *Ministère des Armées,* janvier 2019.

« Stratégie Nationale du Renseignement », Coordination Nationale du Renseignement et de la Lutte contre le Terrorisme, Paris, Ministère de l'Intérieur, juillet 2019

Royaume-Uni

« Cyber Primer » 2nd ed., *Development, Concepts and Doctrine Centre, United Kingdom Ministry of Defense* Shrivenham, Wiltshire, juillet 2016.

Contact : iesd.contact@gmail.com

Site : https://iesd.univ-lyon3.fr/

IESD – Faculté de droit
Université Jean Moulin – Lyon III
1C avenue des Frères Lumière – CS 78242
69372 LYON CEDEX 08