L'art de la guerre dans un monde hyperconnecté

Lionel Meny

Colonel (terre), auditeur de la 70e session du Centre des hautes études militaires (CHEM).

Le concept de guerre en réseau n'est pas nouveau. Depuis les années 2000, les armées, dans le sillage des doctrines américaines de *Network Centric Warfare* (*NCW*), se sont engagées dans la numérisation du champ de bataille. Force est de constater que cette transformation s'est heurtée autant à des limitations techniques, qu'à de fortes résistances « sociales ». Plus encore, la numérisation s'est déployée comme un outil technologique en appui des états-majors, une réponse technique pour tenter d'organiser le chaos des informations et gagner en supériorité opérationnelle. Pour autant, elle n'a conduit ni à de profondes réformes structurelles des états-majors, ni à de grandes adaptations des doctrines tactiques. En clair, nous avons globalement réussi à faire mieux, plus vite et plus précis, mais sans chercher à faire autrement pour en exploiter toutes les opportunités.

Aujourd'hui, nous entrons dans une tout autre dimension, celle de l'hyperconnectivité. Elle résulte de la conjonction de nombreuses technologies (réseau, *Data*, Intelligence artificielle – IA –, automatisation, *Internet* des objets – *IoT*), ainsi qu'une transformation des usages majoritairement tirés par le secteur civil. Elle porte la promesse, tant pour des usages privés que professionnels, d'une mise en relation permanente, intuitive et interactive des individus, des machines et des données dont le volume croît de manière exponentielle. Deux repères pour mesurer ce que cette révolution recouvre dans notre quotidien : la technologie *4G* était capable de soutenir de l'ordre de 60 000 « objets connectés » au kilomètre carré, demain la *5G* en soutiendra près d'un million ; et 24 milliards d'appareils disposant de senseurs connectés en réseau sont aujourd'hui opérants dans le monde [(1)].

Dans un tel contexte, alors que l'hyperconnectivité innerve toute l'épaisseur de la chose militaire, du niveau stratégique au niveau tactique, comment en tirer tous les avantages et se prémunir des vulnérabilités qu'elle induit ? De par sa dimension globale, aussi technologique que sociétale, elle constitue une rupture qui transforme les espaces de conflictualité, bouleverse les notions de surprise et questionne la place de l'homme dans la guerre. Du niveau stratégique au niveau tactique, il s'agira d'analyser ce que recouvre l'hyperconnectivité, d'en déduire dans quelle mesure elle modifie certains principes fondamentaux de la guerre et d'en tirer quelques préconisations.

(1) Institute for the Future, *The Hyperconnected World of 2030–2040*, 2020, 85 pages (https://www.iftf.org/).

L'hyperconnectivite, un nouveau paradigme stratégique

De par son caractère global, fortement intriqué, l'hyperconnectivité, avant d'être un phénomène technologique, constitue d'abord un phénomène sociopolitique qui touche toute la société. Ensuite, elle modifie le rapport entre les individus, en influence les perceptions et, d'une certaine manière, pervertit les cycles de décisions politico-militaires. Elle contribue, par ailleurs, à modifier l'appréhension de la conflictualité.

Une transformation avant tout sociopolitique porteuse de fragilités (le levier de la guerre d'influence)

Lorsque l'on cherche le mot hyperconnectivité sur *Internet*, ce sont prioritairement les études sociologiques et les articles de neurosciences qui constituent la majorité des pages proposées, preuve que ces deux aspects constituent clairement un enjeu majeur. En comprimant les temps et d'une certaine manière l'espace, en modifiant les équilibres sociaux et en agissant en permanence sur les facultés cognitives tant individuelles que collectives, l'hyperconnectivité impacte significativement la liberté d'action politique.

• Un catalyseur des communautarismes qui favorise les fractures et pose la question de la cohésion sociale…

Par construction, l'hyperconnectivité, qui permet la mise en relation de l'ensemble des individus, porte l'illusion qu'elle va les rapprocher. L'identité réelle se fond progressivement dans une identité virtuelle poussant les individus à se raccrocher à des communautés d'intérêt de tous ordres, et ce d'autant plus facilement que les algorithmes des réseaux sociaux le favorisent. En outre, la multiplication des objets personnels connectés, déployés jusque dans l'intimité, est autant de capteurs de données qui viennent enrichir ces mêmes algorithmes.

Par voie de conséquence, se développent de nouvelles allégeances parfois très éloignées de l'intérêt général ou du sentiment d'appartenance à la nation. Or, ce phénomène touche indistinctement toute l'épaisseur de la couche sociale, comme a pu le révéler l'analyse de l'émergence du mouvement des Gilets jaunes [(2)].

Il devient ainsi aisé pour un adversaire, d'exploiter ces fragilités en vue de déstabiliser nos sociétés, d'en fragiliser la cohésion ou d'en infléchir l'adhésion aux institutions et leurs représentants.

• Qui exploite les biais cognitifs…

La permanence, la redondance et la sur-sollicitation qui accompagnent l'hyperconnectivité induisent, par ailleurs, des troubles cognitifs qui influent directement sur les capacités de choix, de décision et de réflexion, au point que le sociologue Gérald Bronner parle « d'apocalypse cognitive » [(3)].

[(2)] Bartlett Jamie, « L'homme ou la machine ? Comment *Internet* tue la démocratie (et comment la sauver) », *Interfaces numériques*, vol. 9 n° 1/2020, 2019, De Boeck Supérieur (https://www.unilim.fr/interfaces-numeriques/4179&file=1).
[(3)] Bronner Gérard, *Apocalypse cognitive, la face cachée de notre cerveau*, Puf, 2021, 372 pages.

Plusieurs études conduites au sein d'entreprises révèlent que la surinformation a non seulement eu des effets néfastes sur la créativité des collaborateurs, mais les conduits à ne traiter les informations que dans l'urgence, les empêchant de se projeter dans le temps long et de conserver le cap d'une stratégie établie. En outre, s'activent dans ces conditions les mécanismes de la récompense qui rendent les cerveaux particulièrement sensibles aux biais de confirmation et émoussent esprit critique et volonté.

Ce biais constitue une forte vulnérabilité, tant individuelle que collective, aux opérations d'influence et aux intoxications [4], qui peuvent notamment être exploitées pour pervertir les cycles de décision.

- **En modifiant la perception du temps et de l'espace.**

De plus, l'hyperconnexion conduit à fausser la notion de temps [5]. Chaque nouvelle information venant chasser la précédente entretient le sentiment d'urgence. Par ailleurs, en touchant toute la chaîne de la société, elle implique immédiatement et simultanément le décideur autant que le citoyen, ne laissant aucune place à l'analyse, la mise en perspective et le recul.

Par voie de conséquence, les échelons de décision sont soumis à une pression permanente qui les conduit à devoir réagir dans des délais contraints et à expliciter publiquement les actions entreprises. Ceci bouleverse les cycles de décision, d'élaboration et de suivi des stratégies. Sur le plan de l'engagement militaire, ce phénomène se traduit par une forme « d'impatience stratégique » doublée d'une « fascination tactico-technique ».

Enfin, elle bouleverse le rapport à l'espace en faisant entrer les événements les plus éloignés dans l'intimité des individus, ce qu'Étienne Klein [6] appelle la « téléportation de la présence » [7].

Qui a pour conséquence de modifier le périmètre de la conflictualité et de bouleverser les notions d'avant et d'arrière

Dans ce contexte marqué par la prééminence et la permanence de l'information, ainsi que par les vulnérabilités sociétales induites par l'hyperconnectivité, les actions à l'avant ne peuvent être décorrélées de la sûreté et de la stabilité à « l'arrière ». Les adversaires infra-étatiques chercheront ainsi la furtivité face à la supériorité technologique et informationnelle en important leur combat au sein même de nos sociétés. Les compétiteurs étatiques pratiquant les stratégies d'ambiguïté chercheront à exploiter

---

[4] Dans leur étude influence 2.0 – comprendre les opérations d'influence dans un monde hyperconnecté – Jean Caire et Sylvain Conchon explicitent clairement comment les sur-sollicitations numériques constituent des fragilités qui peuvent être exploitées, notamment dans les cycles de prise de décision.

[5] Bouton Christophe, « À la recherche de l'espace. Hyperconnexion, rapprochement et dé-localisation », *@ la recherche du temps*, 2018, p. 151-168.

[6] Directeur du laboratoire de recherche sur les sciences de la matière au Commissariat à l'énergie atomique et aux énergies alternatives (CEA).

[7] Colonel (r) Mirikelam François, « La guerre à distance(s), une réalité qui s'impose. Gagner au contact », *Pensée Militerre*, CDEC, 10 mai 2019 (https://www.penseemiliterre.fr/).

les dépendances et fragilités induites par l'hyperconnexion en s'attaquant directement aux individus dans le champ informationnel.

Les opérations d'influence pourront toucher indistinctement l'arrière aux fins de déstabilisation et de manipulation, pour peser sur la volonté politique, comme ce fut le cas il y a quelques mois dans le contexte des tensions avec la Turquie [8]. Elles pourront se déployer également directement à l'encontre des soldats ou de leur environnement (familles notamment) en exploitant leur surface numérique. Lors de la campagne russe en Ukraine, des militaires ont ainsi reçu des SMS leur indiquant qu'ils étaient « encerclés ». Simultanément, leurs familles avaient reçu des messages les informant que leurs proches étaient morts. L'analyse des échanges téléphoniques entre familles et soldats avait permis de géolocaliser les unités et de les attaquer avec des frappes d'artillerie [9].

En outre, nos dépendances aux réseaux pourront être exploitées par le biais d'attaques cyber ciblées visant à décrédibiliser, interdire l'accès à certains services, fausser nos appréciations, paralyser les approvisionnements. En juin 2017, suite à la mise à jour d'un logiciel ukrainien, le code malveillant *NotPetya* se diffuse en Europe à des fins de sabotage. Il touche plus de 2 000 sociétés dont le groupe danois Maersk, contraint d'interrompre le fonctionnement de certaines de ses activités.

Toute intervention hors du territoire national ou toute projection de puissance aux fins d'intimidation devront, par conséquent, être conçues en tenant compte des possibilités d'exploitation et de contre-mesure de la part de nos adversaires sur le territoire national. Cela nécessitera d'un côté, une volonté politique forte pour résister aux opérations de déstabilisation et d'influence, et de l'autre, une communication robuste de nature à contrer les désinformations. Les dispositifs actifs et passifs de protection de nos réseaux et systèmes devront être renforcés. Enfin, il s'agira de disposer de moyens susceptibles d'être déployés sur le territoire national en cas de dégradation.

À l'avant, il faudra pouvoir afficher des dispositifs crédibles et dissuasifs de nature à peser sur les volontés adverses.

Quelle stratégie déployer ?

La réponse à ce nouveau paradigme de conflictualité, repose sur une stratégie de moyens, la crédibilité militaire et sur le développement de stratégies de posture. Sur le plan technologique, trois domaines sont de nature à constituer une plus-value en appui des stratégies militaires, tant offensives que défensives. Ils font l'objet d'un effort marqué au sein du ministère des Armées comme l'illustrent les différents discours cadre ministériels.

- Les technologies de l'intelligence artificielle doivent non seulement apporter des gains significatifs dans le domaine de la surveillance des réseaux, mais aussi

[8] AFP, « La France dénonce "les tentatives de déstabilisation" », *L'Orient-Le Jour*, 28 octobre 2020.
[9] Collins Liam (colonel), « Russia gives Lessons in Electronic Warfare », *Association of the United States Army* (*AUSA*), 26 juillet 2018 (https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare).

améliorer le fusionnement et l'analyse des données en vue de faire émerger une capacité d'analyse prédictive. L'enjeu est défensif, en favorisant l'identification de signaux faibles qu'ils soient d'ordre cyber (*malware*, *hacking*) ou d'ordre informationnels (identification des paquets d'informations ou des constitutions de groupes sociaux…). Il l'est aussi dans une perspective offensive, en améliorant la compréhension des systèmes adverses en vue, le cas échéant, de les cibler.

• Les technologies de la donnée recouvrent trois domaines clés : celui de l'hébergement et de la protection (être souverain), celui du fusionnement et de l'exploitation (exploiter) et celui de la fiabilité. Or, la question de la fiabilité constitue un enjeu majeur du développement de l'IA et du *deep learning* [10], en particulier [11]. Elles sont vulnérables à trois grands types d'attaques, l'empoisonnement, l'évasion et l'interférence. Les données doivent ainsi être considérées, elles aussi, tant du point de vue défensif qu'offensif. Ainsi, le cyber constitue autant un bouclier, qu'un levier « cinétique » et un facilitateur des opérations d'influence.

Pour peser dans cette nouvelle conflictualité qui va de la compétition à l'affrontement, il s'agit d'être craint et respecté. Cela passe notamment par la démonstration permanente de notre crédibilité opérationnelle, dans les champs matériels et immatériels. Cette crédibilité s'inscrit dans une forme de dialectique de puissance qui s'appuie sur les résultats opérationnels de nos engagements, mais doit être complétée de stratégies de postures. Celles-ci peuvent notamment s'appuyer sur des déploiements inopinés de forces (renforcements ponctuels de nos dispositifs prépositionnés ou de souveraineté), des exercices de grande envergure sur et hors du territoire national, des démonstrations de l'épaisseur de nos forces (réserves, remontées en puissance). En outre, ces démonstrations de puissance doivent être consolidées, idéalement coordonnées, par des postures similaires dans les champs immatériels (cyber, sphère informationnelle), soutenues par une communication stratégique (*StratCom*) assumée et endossée par le politique. C'est, entre autres, l'objectif poursuivi par le premier exercice spatial, *Aster X* [12], qui s'est déroulé du 9 au 12 mars 2021. Le cas échéant, elles doivent pouvoir être combinées avec des exercices impliquant les capacités de dissuasion.

Enfin, ces stratégies de posture nécessiteront de renouveler le processus de décision politico-militaire. Pour adapté qu'il est aux engagements aujourd'hui, très contenus et localisés, il devra répondre à la dimension globale du dialogue stratégique avec un compétiteur symétrique qui agit sur tout l'éventail de la conflictualité. Il s'agira, entre autres, d'associer plus largement l'ensemble de la sphère interministérielle pour traiter des stratégies, tant de défense à l'arrière que d'action à l'avant. Ces processus

---

[10] Les systèmes de *deep learning* peuvent améliorer leurs performances en accédant à davantage de données : une machine plus expérimentée.

[11] « Dans le cas de **l'empoisonnement**, un attaquant cherche à biaiser le comportement d'un modèle en modifiant les données d'apprentissage. Avec **l'évasion**, un attaquant joue sur les données d'entrée de l'application afin d'obtenir une décision différente de celle normalement attendue. Enfin, dans le cas **l'inférence**, un attaquant teste successivement différentes requêtes sur l'application afin d'étudier son comportement. » Biseul Xavier, « Comment sécuriser le *machine learning* », *JDN*, 25 novembre 2020 (www.journaldunet.com/).

[12] Il réunit tous les services civils et militaires participant à la protection de l'Espace, autour d'un thème allant du risque de retombées de débris menaçant la population, à l'attaque d'un satellite par un adversaire en vue de le neutraliser.

devront, par ailleurs, faire l'objet d'entraînements, de mise en situation et de *war-gaming* [13].

L'hyperconnectivité, un amplificateur de l'art opératif

L'art opératif consiste, selon le maréchal britannique Montgomery, à « rendre tactiquement possible ce qui est stratégiquement désirable » [14]. Il s'agit donc du niveau de traduction de l'intention politique en actions miliaires intégrées, coordonnées et synchronisées, sur l'ensemble du spectre des opérations. Ce que consacre le concept américain du « *Multi Domain Operations* ». L'idée de *Network Centric Warfare* [15] a apporté une première réponse technique à ce besoin de contrôle des opérations. Elle a favorisé l'émergence de la situation opérationnelle partagée (*COP*, *Common Operational Picture*) et a renforcé la synchronisation et la coordination des opérations dans les 3 dimensions (concept d'*Air-land Battle*). Cette évolution, dans un contexte de forte domination technologique occidentale sur les adversaires, a conduit à développer une vision très linéaire et cinétique des engagements, principalement centrée sur l'attrition.

Or, l'hyperconnectivité laisse entrevoir un changement radical de dimension notamment au travers de ses technologies connexes (la connectivité, les technologies de la donnée et l'IA). En outre, elle conduit à repenser l'idée de surprise et nécessite une réflexion sur la structure et le fonctionnement des états-majors pour être pleinement exploitée.

La fonction fédératrice des technologies connexes de l'hyperconnectivité donne toute sa plus-value au niveau opératif…

Dans les trois domaines d'excellence du niveau opératif – compréhension, synchronisation et décision –, les technologies connexes de l'hyperconnectivité constituent un levier amplificateur significatif.

Les technologies de la connectivité permettront, en effet, la mise en relation de l'ensemble des plateformes présentes sur le champ de bataille, ainsi que des opérateurs. Chacune sera alors en mesure de capter, diffuser et exploiter les données collectées [16]. On peut aisément imaginer les gains en matière de renseignement où cette multitude de sources pourra apporter une réponse aux problématiques de la permanence et de la dimension de l'espace de bataille. De même, les performances des chaînes logistiques et de maintenance devraient être améliorées par les remontées permanentes d'informations qui favoriseront anticipation des flux et planification des opérations de soutien.

---

[13] À l'image du « *Global-Game* » BSS (Bande sahélo-saharienne) qui s'est tenu en 2020 et regroupait l'ensemble des acteurs interministériels impliqués dans la résolution de la crise au Sahel.

[14] Desportes Vincent, « La stratégie en théories », *Politique étrangère*, vol. 2014/2 (Été), p. 165-178 (https://www.cairn.info/revue-politique-etrangere-2014-2-page-165.htm).

[15] Concept américain issu de la première guerre du Golfe et fondé sur l'idée de la conduite des opérations en s'appuyant sur le partage de l'information et l'exploitation des réseaux informatiques.

[16] À l'image du *F-35* qui constitue une véritable plateforme multidomaines intégrant, en temps réel, l'ensemble des informations du champ de bataille.

Les technologies de la donnée permettront de développer les solutions telles que les « *Data as a service* » (*Daas*) [17] et les plateformes numériques qui assureront aux états-majors d'accéder à une information fusionnée, triée et plus facilement exploitable. Ce champ constitue le cœur de la plus-value de l'hyperconnectivité pour les échelons opératifs, autant que le principal défi. S'il porte la promesse d'une meilleure compréhension des situations et des systèmes adverses, il devra résoudre la question de la granularité de l'information, de son accessibilité et de sa fiabilité. Jusque-là, les développements de la numérisation de l'espace de bataille et du combat info-centré n'y ont pas complètement répondu.

Les technologies de l'IA devraient, elles, améliorer les processus de planification et de conduite. L'exploitation automatisée des données de masse permettra de dégager des tendances et d'en déduire des opportunités d'engagement. *A minima*, cela contribuera à réduire les boucles décisionnelles et à apporter un appui à la discrimination des objectifs. Le *deep learning* devrait donner aux machines des capacités accrues d'analyse prédictive. On peut ainsi imaginer qu'elles seront capables non seulement d'envisager les modes d'actions adverses, mais aussi de proposer des options pour nos propres actions.

En synthèse les technologies de l'hyperconnectivité devraient, d'une part, favoriser une approche multidomaine des opérations, raccourcir et optimiser les chaînes décisionnelles (*Kill Chain*) et, d'autre part, contribuer à lever le brouillard de la guerre, sur les amis, les adversaires et l'environnement.

L'hyperconnexion bouleverse les notions de surprise et d'imprévisibilité

Dans un contexte de compétition dans le segment haut de la conflictualité, ces technologies constituent autant un avantage qu'elles portent une fragilité.

Dans un espace de bataille réputé transparent, la notion de surprise et d'imprévisibilité se trouvera bouleversée. La multiplicité des capteurs techniques, au même titre que les activités humaines laisseront peu de libertés à la discrétion des déploiements qui seront plus lisibles. Le site Liveuamap.com (toujours actif) exploitant les réseaux sociaux et les informations qui y circulent recense ainsi minutieusement les activités militaires dans le monde.

Or, dans le prolongement des stratégies globales de postures décrites plus haut, la capacité à générer la surprise et à être imprévisible constitue un facteur de crédibilité autant que de succès opérationnel. « Ce n'est ni par la façon de s'armer, ni par celle de se ranger qu'Hannibal a vaincu : c'est par sa ruse et sa dextérité [18]. » Pendant la Seconde Guerre mondiale, l'opération *Fortitude*, qui a consisté à intoxiquer l'état-major allemand pour lui faire croire à un débarquement dans le Pas-de-Calais constitue un modèle du genre [19], combinant les trois leviers de la déception : dissimulation,

---

[17] L. Bastien, « Data as a Service : qu'est-ce que c'est et à quoi ça sert ? », *Le Big Data*, 30 novembre 2018 (https://www.lebigdata.fr/data-as-a-service-definition).

[18] Maurice de Saxe.

[19] Ont ainsi été combinées la constitution d'unités fictives, la simulation d'activités radio intense, des fuites organisées vers les réseaux diplomatiques et de renseignement.

intoxication et simulation. D'une certaine manière, la technologie apportera une partie de la réponse pour générer la surprise. La précision des armes et l'amélioration conjuguée des portées et de leur vélocité permettront de délivrer des frappes ciblées sur les centres de gravité adverses pour générer neutralisation et sidération.

Des systèmes autonomes, fonctionnant en essaim sont capables de simuler les signatures électromagnétiques d'unités ou de moyens, dans le but de leurrer les défenses adverses ou d'intoxiquer les états-majors. Le *MALD* [20] (*Miniature Air-Launched Decoy*) américain est ainsi employé en avant des raids aériens. Il simule la signature de tout type d'aéronef pour saturer les défenses sol-air adverses et fausser les analyses de situation des états-majors ennemis. Les évolutions technologiques devraient vraisemblablement permettre de réduire les coûts d'acquisition de ce type de système et d'en généraliser l'usage.

Il s'agira, par ailleurs, d'agir sur les échelons de décision adverses. On pourra ainsi saturer les états-majors en multipliant les fausses informations (intoxication, simulation). L'exploitation de la surface numérique des individus pourrait permettre d'identifier les décideurs, de comprendre leur mode de pensée en vue de les déstabiliser. Les opérations cyber pourront directement viser l'intelligence artificielle de l'ennemi en cherchant à en fausser les analyses. Une équipe de chercheurs de Google a ainsi montré qu'il était possible de biaiser les systèmes de reconnaissance d'image en utilisant le système des « exemples adverses [21] ».

En clair, il faudra exploiter les leviers qu'offre l'hyperconnectivité pour donner aux opérations de déception toute leur envergure, en les combinant avec la juste articulation des dispositifs et des forces. Dans ce cadre, il sera peut-être nécessaire de réétudier le volume de nos engagements pour pouvoir générer des forces de déception crédibles.

Une nécessaire adaptation des systèmes de commandement

La permanence et le flux des informations générés par l'hyperconnectivité et la globalité dès l'engagement multidomaine devraient conduire à une forte sollicitation des états-majors au risque de les saturer. Il s'agira donc, non seulement de garantir le « tri » des informations qui remonteront aux états-majors, mais aussi leur exploitation. On peut envisager que la machine puisse, dans ce domaine, apporter un appui par le traitement automatisé de certaines données. Le regroupement sur un réseau informationnel unique de l'ensemble des niveaux devrait également faciliter l'acheminement des informations pertinentes et rafraîchies.

En outre, la dimension, l'immobilité et le rayonnement électromagnétique font des états-majors, des cibles privilégiées d'attaque tant cinétiques que cyber ou

[20] Le programme *MALD* américain a été lancé en 1995 et a débouché sur les premières livraisons du système Raytheon *ADM-160B* en 2009.

[21] Il s'agit de superposer sur l'image un réseau de pixels imperceptibles à l'œil nu et qui trompe l'intelligence artificielle. Dans cette expérience, où l'on proposait une image de panda systématiquement reconnue avant leurrage, l'IA reconnaissait immanquablement un gibbon après adjonction du *malware*.

informationnelles. Dans les années 1960, un PC de division comptait de l'ordre de 250 personnes, aujourd'hui ses effectifs s'élèvent à près de 500, installés dans une cinquantaine d'abris préfabriqués de commandement. La faible modularité des systèmes d'information et les contraintes de déploiement nécessitent des délais d'installation dépassant la semaine. Dans ce cadre, l'hyperconnectivité pourrait apporter des solutions techniques, en favorisant l'éclatement « géographique » des PC. Les technologies de transmission de données optiques pourraient contribuer à réduire significativement le rayonnement électromagnétique [22], autant qu'à alléger les charges d'installations [23]. Plus généralement, une réflexion sur les plateformes mobiles de PC pourrait être menée pour redonner aux états-majors de la mobilité.

La compression des cycles de décision, la rapidité probable des engagements nécessiteront de pouvoir concilier davantage réflexion, conception et conduite sans perdre la cohérence et la collusion intellectuelle. Certaines fonctions pourraient être conduites de manières délocalisées ou en *reach back*. Une partie du traitement du renseignement pourrait ainsi être conduite à l'arrière en recourant à l'IA, comme cela a été expérimenté dans le cadre de l'opération *Barkhane*. La *Red Team*, constituée au sein de la Direction du renseignement militaire (DRM), produit ainsi des analyses systémiques, des cartographies adverses qui permettent au Poste de commandement interarmées de théâtre (PCIAT) de mieux cibler les zones d'application de ses opérations.

Les états-majors devront en plus disposer de nouvelles compétences de nature à mettre en cohérence et en convergence le champ immense de la donnée. Elle pourrait constituer une fonction opérationnelle particulière d'appui numérique, dont le périmètre comprendrait à la fois la fiabilisation des données, les politiques de fusionnement et la cohérence des systèmes d'information [24].

Enfin, il s'agira de changer de « *mindset* » (mentalité) au sein de nos états-majors, pour retrouver le chemin de la créativité, le goût de la ruse et l'aptitude à sortir des carcans de procédures et de schémas. L'imprévisibilité se gagnera certes avec le recours à la technologie, mais comme appui à une pensée manœuvrière. Dans ce cadre, la sélection des officiers d'état-major, autant que les méthodes de raisonnement opérationnel très « linéaires » pourraient s'ouvrir à des profils plus « atypiques » et des modes de réflexions plus créatifs [25].

---

[22] Développées au cours des années 2000, les liaisons sol-Espace par laser arrivent à maturité, le Projet européen *EDRS* (*European Data Relay Satellite System*) est en cours de déploiement.

[23] Les technologies de *LIFI* (*Light Fidelity*), testées en 2019 au sein de l'EM de la 4e Brigade d'aérocombat (BAC) permettent en particulier de réduire significativement le volume de câbles et de gagner en délais d'installation du PC.

[24] Rolland Erwan, « L'intégration et l'appui numérique : la nouvelle fonction opérationnelle du combat du futur », *RDN* n° 833, octobre 2020, p. 71-80.

[25] L'expérience récente de sous-chef opération a montré à quel point les méthodes traditionnelles de réflexion « tactique » sont finalement peu adaptées pour exploiter parfaitement les opportunités dans le domaine des actions dans les champs immatériels. Des méthodes inspirées de celles enseignées par Ivan Gavriloff et Jarrosson Bruno dans leur ouvrage *Une fourmi de 18 mètres ça n'existe pas* (3e édition, Dunod, 2011, 240 pages), pourraient opportunément les compléter.

Le niveau tactique, le défi humain de l'hyperconnectivité

Le niveau tactique n'échappe pas aux transformations induites par l'hyperconnectivité. Dans une certaine mesure, c'est vraisemblablement à ce niveau que ses effets, positifs ou non, ont été les plus testés, analysés et, finalement, traduits en doctrine. Le retour d'expérience de vingt ans de tentative laborieuse de numérisation et, plus récemment, les expérimentations conduites dans le cadre de l'appropriation du programme *Scorpion* (*Synergie du contact renforcée par la polyvalence et l'infovalorisation*) ont permis de disposer d'une vision assez large des bénéfices tactiques à attendre, autant que des fragilités.

Bien que la dorsale de l'hyperconnectivité soit avant tout technologique, c'est au final les défis humains – et singulièrement la place de l'homme – qui sont au cœur de cette transformation.

Masse–initiative–manœuvrabilité : les promesses de l'hyperconnectivité tactique

L'infovalorisation devrait permettre des gains significatifs de trois ordres : accélération, agressivité et plasticité.

L'effet de masse pourra être gagné par des systèmes jouissant d'une relative autonomie, combiné à la précision et la brutalité des feux. Le récent conflit au Haut-Karabagh a ainsi mis en lumière la plus-value que pouvait apporter l'usage de drones suicides, en particulier pour saturer les défenses aériennes adverses [(26)]. L'Agence [américaine] pour les projets de recherche avancée de défense (*DARPA*) développe de son côté le concept de *Mosaic Warfare* qui combine moyens conventionnels et essaims de drones aux capacités complémentaires et interconnectées [(27)].

La mise en commun des capacités de frappes, notamment dans la profondeur, permet d'envisager une capacité de destruction accrue des unités tactiques. La notion d'appui indirect devrait ainsi être totalement renouvelée par son intégration croissante dans les 3 dimensions. Reliées par le même réseau, les unités d'appui bénéficiant d'une mise à jour en temps réel de la situation tactique sont ainsi capables d'anticiper leur engagement.

La connaissance quasi-parfaite de la situation amie et l'aide apportée par des systèmes d'aide à la décision permettront au chef tactique de se concentrer sur sa manœuvre. Celle-ci devrait gagner en fluidité tout en étant moins sujette à la friction. La réduction de l'incertitude facilitée par une meilleure intégration du renseignement enrichi par la multitude des capteurs devrait autoriser des dispositifs plus imbriqués. Les unités devront dans ce contexte être plus aptes à se réorganiser, à se ré-agréger pour obtenir localement la concentration et l'économie des forces souhaitées.

[(26)] Jubelin Alexandre, « Une guerre des drones ? Analyse du conflit au Haut-Karabagh », *Le Collimateur*, 20 octobre 2020 (https://www.irsem.fr/).
[(27)] Hambling David, « What Are Drone Swarms And Why Does Every Military Suddenly Want One? », *Forbes*, 1er mars 2021 (https://www.forbes.com/).

Le partage de situation entre les différents niveaux tactiques devrait, par ailleurs, favoriser l'initiative et la subsidiarité, les subordonnés pouvant plus aisément s'imprégner de l'intention du chef ou saisir les opportunités. Ainsi, l'unité tactique interconnectée et agissant dans le cadre général du plan devrait se comporter comme un ensemble cohérent et compact capable de s'adapter aux changements de situation en intégrant les informations transmises par chacun des individus qui la composent. L'échelon de décision, supervisant la manœuvre, verra son rôle de conduite se concentrer sur les éventuelles mesures correctives.

Le combattant lui-même devrait pouvoir bénéficier des apports de l'hyperconnectivité pour améliorer sa perception de l'environnement, discriminer ses adversaires ou visualiser de manière plus intuitive situations tactiques et ordres en cours d'action. Sans présumer des développements portés par la firme Neuralink d'Elon Musk [28], l'augmentation du soldat séduit, d'ores et déjà, de nombreux pays, dont la France qui a formellement défini sa ligne de conduite en la matière [29]. Parmi les technologies les plus immédiatement accessibles, celle de la réalité augmentée est prometteuse. Elle permet au soldat équipé de lunettes, de « plaquer » sur son environnement les informations nécessaires à la conduite de son action, géolocalisation, itinéraires, zones de danger, position des amis… Le programme *IVAS* (*Integrated Visual Augmentation System*), développé par Microsoft pour l'armée américaine, ambitionne en outre d'y intégrer une forme d'intelligence artificielle capable de raccourcir et de « dérisquer » la séquence de ciblage en distinguant objectifs menaçants ou non [30].

Un défi humain, la machinistation

Cette hyperconnectivité du niveau tactique pose principalement un défi autour de la place de l'homme. Dans une certaine mesure, elle conduit à une forme de machinisation [31] de la guerre.

- **Machinisation du feu**

L'automatisation prévisible des boucles décisionnelles et de certains systèmes d'armes, relègue progressivement le rôle de l'homme à celui de « *Red Card Holder* » [32]. Écarté de la phase d'analyse et de choix tactique, sa fonction se réduira à valider le tir ou à en interrompre la séquence s'il juge qu'il n'est pas conforme aux règles d'engagement. Parallèlement, l'amélioration conjuguée de la portée des armes et des systèmes

---

[28] Smith Adam, « US Army Developing Technology That Could Let Soldiers Read People's Minds », *The Independent*, 27 novembre 2020 (https://www.independent.co.uk/)

[29] Délégation à l'information et à la communication de la Défense (Dicod), « Le comité d'éthique de la défense publie son avis sur le soldat augmenté », 8 décembre 2020 (https://www.defense.gouv.fr/).

[30] The Office of the Director, Operational Test and Evaluation, « Integrated Visual Augmentation System (IVAS) », *FY20 ARMY PROGRAMS*, p. 91-93 (https://www.dote.osd.mil/).

[31] Néologisme qui détourne un terme apparu au cours du XIXe siècle décrivant le processus consistant à substituer la machine à l'homme pour l'exécution des tâches répétitives ou de force.

[32] Le *Red Card Holder* assure le contrôle national de la conformité de l'emploi des forces, de l'appréciation autonome de la situation et de l'optimisation de l'emploi possible des aéronefs français. Toute frappe non planifiée effectuée sur un théâtre extérieur est soumise à son approbation.

de détection et de guidage à distance, contribueront à éloigner progressivement le combattant de la zone de létalité des combats.

Si les bénéfices sont évidents, tant sur la performance tactique que sur la protection et l'exposition des soldats, cette désertification du champ de bataille ou, tout du moins, une distanciation de l'homme de la zone de létalité des combats, pourrait avoir des conséquences sur les tabous qui cadrent aujourd'hui le recours à la violence.

- **Machinisation de la décision**

Les technologies de l'IA laissent entrevoir la possibilité que la puissance de calcul et d'analyse des machines parvient à apporter une aide significative aux processus d'élaboration des décisions opérationnelles des états-majors. L'IA pourrait dans ce cadre proposer/préconiser type de manœuvre, dispositif tactique, articulation optimisée des forces… Dans ce contexte, on peut imaginer qu'un choix alternatif, inspiré à la fois par l'intuition et l'expérience humaine, puisse être contesté par les autorités, ce d'autant plus s'il ne produit finalement pas les effets escomptés. À terme, alors que les actions militaires sont de plus en plus décryptées et judiciarisées, pourraient se poser la question de la validité juridique d'un choix tactique qui aurait insuffisamment suivi les préconisations de la machine.

- **Machinistation de l'homme**

Placé au centre d'objets automatisés, appuyé dans ses décisions par l'IA, géolocalisé, équipé de capteurs, connecté numériquement et vocalement, appréhendant son environnement *via* la réalité augmentée, le combattant sera sous la pression de sollicitations (ordres, orientations) et d'informations permanentes. Dans un tel environnement, sa liberté d'action et son initiative pourraient être significativement infléchies et son rôle réduit progressivement à celui d'un simple opérateur de combat, dont « l'intelligence technique » sera prioritairement considérée.

Développer les résiliences

L'hyperconnectivité et le saut technologique qui l'accompagne constituent certainement le ticket d'entrée dans le cadre de la haute intensité, la supériorité opérationnelle qui en est espérée laissant entrevoir un avantage immédiat sur l'adversaire, par la connaissance, l'anticipation et la brutalité qu'elle induit.

Or, on peut aisément admettre que l'adversaire cherchera prioritairement à contourner ou à briser cette supériorité informationnelle en s'attaquant à son épine dorsale, les liaisons. L'espace tactique est vraisemblablement celui où la plus large gamme des moyens d'agression électromagnétique et numérique pourra être déployée. Dans un tel contexte, il faudra être capable de poursuivre le combat, totalement ou partiellement privé de la plus-value opérationnelle de l'hyperconnectivité. Pour s'en assurer, il paraît nécessaire que soient d'emblée cultivées des résiliences.

- **La résilience tactico-technique**

Il s'agira d'une part, de disposer des moyens techniques redondants ou alternatifs permettant de s'affranchir, au moins partiellement, des réseaux et des transmissions

spatiales, y compris dans le domaine de la géolocalisation. Ces résiliences d'ordre techniques, doivent être intégrées d'emblée dans la conception des matériels ; c'est partiellement le cas dans le cadre du programme *Scorpion*.

D'autre part, les unités devront s'entraîner à agir en mode « alternatif » en se privant, pour un temps de la manœuvre, d'un certain nombre de moyens rayonnants en vue de gagner en « furtivité électromagnétique ». Ce choix d'emploi ou non de la largeur de l'éventail technologique devra, par ailleurs, être intégré aux méthodes de raisonnement tactique, comme un des items de la question « avec quoi ».

Les états-majors, qui constitueront des cibles privilégiées, devront apprendre (ré-apprendre) la dispersion, la dissimulation et la mobilité en vue de réduire leur vulnérabilité aux agressions directes, autant qu'aux opérations de déstabilisation qui pourraient être instrumentées dans leur environnement de déploiement. En outre, la structure de commandement devra être capable de s'assurer en permanence du non-dysfonctionnement des systèmes experts et parer les risques d'infiltration, de compromission, de leurrage, de brouillage.

- **La résilience cognitive**

Il s'agira de former les individus de tout niveau à la gestion et l'appréhension de la surcharge informationnelle générée par l'hyperconnexion. Au même titre que sont développées des techniques d'optimisation physique du potentiel, pourraient être développées des techniques d'optimisation du potentiel cognitif.

De plus, les chefs devront cultiver un sens critique pour garantir hauteur de vue et recul face à la virtualisation du combat et aux aides proposées par l'IA, autant que leur aptitude à résister aux intoxications adverses. Les formations aux fonctions d'état-major et de commandement devront intégrer, *a minima*, un volet de sensibilisation aux biais cognitifs et aux manières de s'en prémunir. Les entraînements devront à la fois confronter les états-majors à des adversaires pratiquant la ruse sur un large éventail, et permettre le développement de modes d'actions intégrant les champs les plus larges de la déception.

- **La résilience psychique et morale**

Elle porte, d'une part, sur la capacité à résister aux opérations d'influence et aux manipulations, notamment amplifiées par les réseaux sociaux et sur lesquels soldats et familles sont particulièrement vulnérables. Sommes-nous en effet collectivement prêts à résister à une intoxication telle que l'ont connue les parents des soldats ukrainiens à qui on annonçait la mort de leurs enfants ? Des séances de sensibilisations sont, d'ores et déjà, régulièrement conduites à destination des militaires et de leurs proches. Mais dans le contexte d'un conflit de haute intensité, où les opérations de déstabilisation et de désinformation seraient massives, il pourrait être envisagé de mettre en place une structure dédiée, capable de détecter et de réagir dans des délais courts pour délivrer la juste information.

D'autre part, face à une forme de virtualisation de la guerre, de déshumanisation du feu, il s'agira de cultiver un sens éthique de nature à garantir de vaincre sans perdre son âme.

Enfin, dans le cadre du combat collaboratif, propice aux changements rapides de postures et d'articulation tactique, le combattant pourra ressentir un effet d'isolement et de « déracinement » de ses références. Ce phénomène sera renforcé par le recours plus systématique aux transmissions numériques au détriment du contact physique et vocal. La place des chefs et leur style de commandement au combat devront s'adapter à cette nouvelle réalité, et les entraînements développer les forces morales pour y résister.

⁂

L'hyperconnectivité est un phénomène social qui irrigue les sociétés jusqu'à en modifier les équilibres et en fragiliser la cohésion. En favorisant la permanence et l'immédiateté de la diffusion de l'information, elle fait entrer la guerre dans la cité. Exploitée à des fins de manipulation et d'influence comme un extraordinaire « cheval de Troie », elle contribue à la globalité de la conflictualité, fragilisant l'arrière. En outre, remarquable levier technologique, elle permet l'interconnexion d'une multitude de capteurs, la collecte et la synthèse d'un volume inégalé de données, jusqu'à lever le brouillard de la guerre. En ce sens, elle remet profondément en question les notions d'imprévisibilité et de surprise consubstantielles au succès opérationnel. Enfin, ses apports dans le domaine de l'aide à la décision, de l'automatisation du feu, tendent à éloigner progressivement l'homme de la létalité des combats par un phénomène de « machinisation de la guerre ».

Or, dans le contexte de retour des dialectiques de puissance allant de l'intimidation à la confrontation, face à des adversaires qui chercheront alternativement la furtivité ou la démonstration de force, pratiqueront ambiguïté et fait accompli, et exploiteront tout l'éventail de la conflictualité, le levier que constitue l'hyperconnexion invite à développer de nouvelles stratégies. Au niveau stratégique, elles devront susciter crainte et respect en combinant postures militaires et *StratCom* assumée, appuyées par un processus de décision politico-militaire renouvelé et élargi. Au niveau opératif, il s'agira plus que d'exploiter le levier technologique, de retrouver le chemin intellectuel de la manœuvre, de la ruse et de l'imprévisibilité. Enfin, il s'agira de pouvoir dépasser les fragilités consubstantielles de l'hyperconnectivité en développant une véritable culture de la résilience, technique, cognitive morale et physique. ◆