

NOTE DE RECHERCHE

LTN (R) Calixte WAGNER
Pôle études et prospective /
Bureau anticipation et innovation

22/05/2024

« L'héritage du *Galactica* » : une analyse des défis et vulnérabilités induits par la technologie au sein de l'armée de Terre.

Ce document ne constitue pas une position officielle de l'armée de Terre.

Résumé

Dans le sillage des concepts de « Révolution dans les affaires militaires », d'« opérations basées sur les effets » ou encore de « démarche capacitaire », la technologie est encore perçue comme une solution prometteuse à la plupart des défis du combat aéroterrestre. Cependant, les enseignements des conflits récents en Ukraine ou au Proche Orient, de même qu'une analyse sommaire des systèmes d'armes les plus technologiquement avancés, qui mettent en œuvre les principes d'autonomisation ou encore de robotisation, nous invitent plutôt à considérer un certain nombre de vulnérabilités.

Il s'agit tout d'abord du constat de l'asymétrie de l'emploi de systèmes d'armes très technologiques et onéreux pour frapper des objectifs à faible coût, ce qui interroge quant à la capacité de maintenir un tel modèle dans la durée d'un conflit de haute intensité. La technologie ne peut être une fin en soi des programmes d'armement futurs : elle ne permet pas encore de pallier le manque d'effectif, voire nécessite du personnel spécialement qualifié (opérateurs, maintenanciers, etc.) ; elle suppose des infrastructures dédiées toujours plus importantes et capables d'assurer le traitement des données (notamment en ce qui concerne l'infovalorisation) ; elle peut entraîner une perte de savoir-faire des soldats qui prennent l'habitude d'une externalisation de certaines actions.

En réponse aux défis futurs, la prise en compte de ces nouvelles vulnérabilités, à la mesure des nouvelles technologies, tout autant que le besoin d'une forme d'équilibre (« *high-low mix* ») à retrouver seront essentiels. À ce titre, la maîtrise d'un « mode dégradé permanent », prenant en compte « l'expérience-utilisateur » pourrait être une piste pour affronter la perspective d'un conflit de haute intensité dans le cadre d'un environnement de combat où chaque civil connecté sera une cible ou une menace.



Synthèse pour le lecteur pressé.

À partir du postulat de la prééminence de la technologie parmi les solutions envisagées pour le combat aéroterrestre futur, la présente étude cherche à mettre en exergue les limites d'un tel recours comme fin en soi en s'appuyant tout à la fois sur une analyse des systèmes d'armes les plus sophistiqués (robotique, intelligence artificielle) et sur les enseignements des conflits les plus récents (Ukraine, Haut-Karabakh, Proche-Orient).

Plusieurs éléments sont soulignés dans cette étude :

- La technologie ne permet pas encore de pallier le manque d'effectifs. Les nombreux programmes d'armement cherchant à utiliser les innovations les plus récentes multiplient les coûts, et parfois ne sont pas menés à terme pour une utilisation au sein des forces. En outre, la technologie peut provoquer une délégation de savoir-faire qui pourrait se traduire en perte irréversible de capacité opérationnelle ; ainsi, l'emploi de l'IA ou de structures « dronisées » peut conduire à la perte de savoir-faire pour le soldat.
- L'emploi des systèmes d'armes les plus technologiques engendre une perte de résilience pour les unités engagées dans un conflit. À ce titre, les drones sont des cibles aisément traitées (neutralisées ou détruites) et révèlent surtout l'asymétrie entre leur coût de production et celui des armes employées pour les détruire. La quête de l'infovalorisation du champ de bataille met en lumière la perte d'autonomie des échelons tactiques inférieurs ainsi que les faiblesses des infrastructures en charge du traitement des données (besoins importants en bande passante, satellites militaires peu nombreux). Quant à l'intelligence artificielle, l'externalisation de certaines fonctions vers ce type de logiciel peut mener à une perte de savoir-faire tout autant qu'à la création de fragilités dans les outils d'aide à la décision au niveau des états-majors (ex : piratage de l'IA par l'ennemi).
- Le combat aéroterrestre semble refléter l'importance grandissante d'une forme de « *low-tech* » dans laquelle la haute technologie ne serait employée que de manière sporadique tandis que les systèmes d'armes les plus rustiques sont préférés par les soldats. À cela s'ajoute le renforcement d'une hybridation entre civils et militaires, que ce soit par le biais des grandes firmes technologiques (souvent américaines) qui s'assurent d'une expertise dans certains domaines (ex : Palantir dans l'identification de cibles) ou bien avec l'emploi de technologies nivelantes (issues du monde civil) par certains combattants.

Propositions et éléments de réflexion pour l'armée de Terre :

- Orienter la BITD française vers l'idée de « *high-low mix* » avec la production de munitions en masse, la production d'armements plus rustiques et aisés à produire en volume et un concept d'emploi des forces qui considère la haute technologie essentiellement pour la « rupture » en certains moments-clefs des opérations.
- Valoriser un nombre plus restreint de programmes d'armement sélectionnés car ils répondent à la demande des unités tactiques de même qu'au souci de mener les projets à bien (indépendamment des innovations les plus récentes sur le marché civil).
- Développer le concept de « mode dégradé permanent » tant dans l'entraînement des soldats que dans la conception des systèmes d'armes afin de garantir la résilience des uns et des autres en cas de neutralisation de la technologie mise en œuvre.
- Conduire une réflexion d'envergure sur l'intérêt du drone dans les engagements futurs, en privilégiant sans doute la masse de drones *low-cost* pour atteindre les objectifs (avec de potentielles pertes plus acceptables que la perte d'un seul drone de haute technicité ou d'armes plus sophistiquées).
- Développer et déployer les outils nécessaires et adaptés au traitement massif des données issues du champ de bataille (serveurs durcis et redondants possédant une copie locale, moyens de transmission hybrides assurant le débit nécessaire au partage permanent de données, logiciels d'IA déployés dans les états-majors tactiques et pouvant fonctionner sans connexion à un réseau, etc.) pour permettre l'infovalorisation.

Relatant, dans un cadre futuriste et interstellaire, la lutte entre les humains de douze colonies planétaires différentes et des hordes robotiques connues sous le nom de Cylons, la série *Battlestar Galactica* (2003) met en exergue un questionnement sur la notion de « supériorité technologique » dès ses premiers épisodes. Il y est question, après plusieurs décennies d'armistice, d'une attaque coordonnée et généralisée des Cylons sur les colonies humaines qui ne laisse que quelques survivants sur la route d'un exode, tous regroupés autour d'un vaisseau de guerre vétéran, le fameux « Galactica ». C'est précisément son obsolescence technologique – les officiels à bord au moment de l'attaque n'étant présents que pour sa transformation en musée – qui lui vaut sa survie, les centaines d'autres vaisseaux bien plus modernes et performants étant tous détruits après avoir été en proie à leur immobilisation totale (brouillage) par les intelligences artificielles ennemies.

Ce n'est pas un hasard si ce choix scénaristique¹ apparaît dans une série du début des années 2000, soit à l'issue d'une période qui a vu l'émergence puis le développement de ce que l'on a nommé la « révolution dans les affaires militaires » (RAM ou RMA en anglais). Apparue au tout début des années 1990, avec pour corollaire le concept d'« opérations basées sur les effets » (rechercher des « effets à obtenir » plutôt que la destruction de l'ennemi), la RAM a le plus souvent été définie comme un courant de pensée focalisé sur la question des moyens, s'appuyant sur les progrès technologiques particulièrement rapides à l'époque, avec une sorte de foi en la capacité de la science à offrir une large supériorité. L'opération *Desert Storm* en constitue l'ancrage et une forme d'aboutissement, les systèmes de guerre réseau-centrés ayant fourni un avantage aux armées américaines – des systèmes d'armes largement mis en scène dans les médias pour souligner cette supériorité (précision des missiles guidés, imagerie satellitaire, etc.). *In fine*, ce courant aboutit, aux États-Unis de prime abord, à la mise en avant d'une « démarche capacitaire » justifiant l'acquisition de systèmes toujours plus performants et polyvalents – eu égard à la méconnaissance des futures menaces – mais aussi une diminution des effectifs des armées. Une telle situation rappelle la fameuse loi développée par Norman Augustine en 1978 selon laquelle le budget du Pentagone en 2050 ne permettait plus que d'acheter un seul avion tactique².

À l'instar des craintes exprimées par la série télévisée, cette « révolution » a suscité des critiques à partir de l'engagement en Irak en 2003, en particulier de la part du général James Mattis (USMC) expliquant, en novembre 2005 : « *Notre fascination pour la RMA [...] a été une fois encore ébranlée par les leçons de l'histoire nous montrant le rôle essentiel du facteur humain dans la guerre*³ ». Ainsi se fait jour une sorte de « tension » permanente entre la nécessité d'armées bénéficiant d'un apport technologique maximal et l'importance de ce « facteur humain », décliné tout à la fois sur les effectifs, la rusticité, la résilience. Se dirigerait-on vers des conflits où la technologie va dominer l'ensemble des engagements, suivant en cela la perspective d'une « hyperguerre » ouverte par J. R. Allen et A. Husain, dans laquelle les auteurs annoncent la disparition de l'homme du champ de bataille et son remplacement progressif par des machines dopées à l'intelligence artificielle et aux algorithmes – plus performantes et rapides dans la prise de décision ? La question se pose avec d'autant plus d'acuité que l'actualité (enseignements des conflits au Haut-Karabakh, en Ukraine ou au Proche Orient) tend à mettre en avant, de plus en plus, la dynamique

¹ La série *Battlestar Galactica* est un *remake* de celle de 1978 (*Galactica*) dans laquelle l'usage de la technologie supérieure des vaisseaux humains contre eux-mêmes n'est pas présente.

² Voir à ce sujet Damien Wallaert, « La loi d'Augustine est-elle une fatalité pour les armées françaises à 10 ans ? », *Cahiers de la RDN*, « Penser demain », 66^e session du Centre des hautes études militaires, CHEM 2017, pp. 207-220.

³ Cité par le général Vincent Desportes, « Armées : « technologisme » ou « juste technologie » ? », *Politique étrangère*, 2009/2, p. 407.

d'une forme de sobriété technologique (qui économise les coûts et maximise les effets) que l'on comprend le plus souvent sous l'expression de « *low-tech* », de même que le retour de la « masse » (emploi de vieux stocks d'armement). En outre, le développement technologique et technique des matériels militaires nécessite des matériaux et matières premières qui, dès à présent, placent les nations occidentales en situation de vulnérabilité quant à leurs chaînes d'approvisionnement. Cette « insécurité minérale⁴ » pourrait ainsi aussi bien représenter une limite au tout technologique qu'une cause de futurs conflits pour le contrôle des matières premières stratégiques.

La présente étude, ne visant évidemment pas l'exhaustivité, souhaite offrir une approche critique des enjeux et des défis posés à l'armée de Terre par la technologie – au sens des systèmes d'armes novateurs, qui sont souvent qualifiés de « technologie de rupture » – dans la perspective de « futuribles » où la haute-intensité serait l'horizon potentiel des engagements terrestres. Nous reviendrons tout d'abord sur la question du rapport entre masse et technologie, puis nous verrons les tendances actuelles qui forment une sorte de « contre-révolution dans les affaires militaires », et les nouveaux enjeux sous-jacents du développement du « *low-tech* » ou du « *high-low mix* » dans les conflits actuels.

I. L'éternel dilemme entre masse et technologie pour « être et durer » sur les champs de bataille futurs

1. Privilégier la qualité sur la quantité, une illusion persistante ?

Dans ses travaux sur la place de la technologie dans la pensée militaire⁵, la chercheuse Sophie Lefeez a mis en avant les choix qui ont été faits de favoriser le « qualitatif sur le quantitatif ». Elle considère que privilégier le qualitatif au détriment du quantitatif est une erreur dans la mesure où une telle volonté conduit à faire le choix, dans les programmes d'armement, de la polyvalence des systèmes ; or la polyvalence permet d'envisager une multitude d'emplois mais « n'offre pas le don d'ubiquité » sur le champ de bataille. De fait, dans la continuité de la « démarche capacitaire » déjà mentionnée, la recherche des systèmes les plus performants aboutit à une croissance exponentielle des coûts de production et de maintien en condition opérationnelle. Alors que, de manière assez caricaturale, Norman Augustine, ancien sous-secrétaire d'État à la défense américaine (1975-1977), vice-président chez Martin Marietta (1977-1987) et futur PDG de Martin Marietta (1987-1995) puis de Lockheed Martin (1995-1997), annonçait dès 1982 que le budget militaire des États-Unis ne permettrait d'acheter qu'un seul avion de combat en 2054⁶, le général Vincent Desportes soulignait, dès 2009, sa crainte de voir une armée « *high-tech* » dont les matériels seraient contraints à ne pas être employés du fait des coûts d'achat et d'entretien⁷. Il est évident que l'incertitude liée aux futures menaces poussent, notamment le niveau décisionnel, vers des solutions technologiques polyvalentes mais il n'en demeure pas moins que cette ligne politique est susceptible de renforcer, à l'avenir, le « cercle vicieux du paradoxe de l'équipement⁸ ».

⁴ Emmanuel Hache, « Prospective de l'insécurité minérale. Anticiper la nouvelle ère métallique de la transition bas-carbone », *Futuribles*, n° 458, janvier-février 2024, pp. 5-24.

⁵ Sophie Lefeez, *L'illusion technologique dans la pensée militaire*, éd. Nuvis, 239 pages, 2017.

⁶ Norman R. Augustine, *Augustine's Laws*, American Institute of Aeronautics, Inc, New York, 1982.

⁷ Général Vincent Desportes, « Armées...*op.cit.*, p. 410.

⁸ Edward Luttwak, « Les armements peuvent-ils devenir « abordables » ? », *Politique étrangère*, Ifri, 2007/4, p. 777.

Selon ce schéma, le matériel est de plus en plus techniquement avancé, donc de plus en plus cher, ce qui nécessite une spécialisation des soldats qui l'opèrent, donc la diminution des effectifs que vient pallier le surcroît de technologie des nouveaux équipements...

D'une certaine manière, il s'agit également de considérer l'enjeu de l'interopérabilité qui, pensée à tous les niveaux de combat et de commandement, oblige à un alignement sur les normes les plus élevées de l'OTAN, en l'occurrence celles des États-Unis, avec des coûts importants - qui ne peuvent eux-mêmes être amortis qu'avec des économies d'échelle importantes, favorisant ainsi les industriels disposant de commandes publiques nombreuses ou d'une capacité à vendre leurs produits à l'export.



Soldats ukrainiens se positionnant dans une tranchée face aux lignes russes. © Efrem Lukatsky/AP/SIPA

Le retour d'expérience de la guerre en Ukraine invite tout spécialement à reconsidérer ce schéma qui veut que les systèmes viennent pallier le manque d'effectifs. Ainsi, suite à son déplacement sur le terrain, le Dr. Jack Watling, chercheur au *RUSI*, a constaté que l'autonomisation ou la robotisation impliquait davantage de personnel (avec de nouvelles compétences) plutôt qu'une diminution de l'effectif⁹. En effet, l'emploi d'un drone MALE (*Medium Altitude Long Endurance*) comme le *Reaper* requiert deux opérateurs mais au moins une centaine de personnes *a posteriori* pour traiter correctement l'ensemble des données collectées par les senseurs. Par ailleurs, peut-être faudrait-il remettre complètement en question la haute sophistication du matériel au profit d'une masse plus « rustique » dans le cadre d'un engagement conventionnel ? Le général (2S) François Chauvancy¹⁰ a pu avancer ce questionnement vis-à-vis de la situation sur le terrain ukrainien puisque, si la haute technologie permet en théorie de vaincre, elle ne semble véritablement nécessaire que lors de certains moments-clefs (concept « *high-low mix* » sur lequel nous reviendrons). La masse viendrait ensuite exploiter l'avantage, que ce soit dans la saturation adverse ou l'emploi de matériels anciens (chars de plus de 30 ans dans le cas des Russes). Édouard Jolly, chercheur en théorie des conflits armés à l'IRSEM, tire des conclusions assez similaires après un an de conflit, avec une situation qui semble faire la part belle à la masse et au « quasi-rustique » soulignant l'importance des combats de tranchées, de l'artillerie, et du fort besoin en munitions et en chars de bataille¹¹.

⁹ Jack Watling, « Automation Does Not Lead to Leaner Land Forces », *War On The Rocks*, 7 février 2024.

¹⁰ Général (2S) François Chauvancy, entretien avec Alain Juillet sur le thème « Enjeux prospectifs pour la France de la guerre en Ukraine », <https://www.youtube.com/watch?v=TEvOotO4n38>.

¹¹ Édouard Jolly, « Un an de guerre en Ukraine : les quatre armes déterminantes », site du Ministère des armées (defense.gouv.fr), 22 février 2023.

Qu'il s'agisse de nos adversaires potentiels ou de nos alliés, nombreux sont désormais les pays à avoir pris en compte ce retour d'expérience ukrainien dans l'orientation de leur base industrielle de défense à court et moyen termes. Le PDG de l'entreprise d'armement russe Uralvagonzavod, Alexandre Potapov, a confirmé la relance de la production du char T-80 revalorisé (qui n'était plus produit depuis les années 1990) eu égard à son efficacité au combat (d'après le ministère de la défense russe). En Allemagne, le *Bundestag* a voté la relance de production de la mine directionnelle antichar DM22 (en service en 1988 et dont les stocks anciens ont été donnés aux forces ukrainiennes) pour une disponibilité dans la *Bundeswehr* en 2026. Autre exemple avec le contrat du Pentagone pour relancer la production de l'obusier tracté M777 en remplacement de ceux fournis à l'Ukraine – et malgré, semble-t-il, leur vulnérabilité aux munitions téléopérées. En outre, en ce qui concerne les États-Unis, la relance de production de tels systèmes d'armes vient justifier l'abandon d'un programme comme le *Future Combat System* (FCS) de l'*US Army* souffrant d'une dérive des coûts mais surtout d'une inadaptation aux conditions réelles d'engagement (manque de robustesse du fait d'une électronique embarquée trop « fragile »).

2. Éviter la constitution de « cimetières de la technologie »

Les programmes d'armement les plus poussés sont généralement les plus coûteux¹² et semblent « passer par pertes et profits » avant même d'atteindre les forces. À titre d'exemples, nous pouvons mentionner l'abandon du projet d'hélicoptère léger d'attaque et de reconnaissance Comanche ou encore l'abandon du programme d'équipement TALOS pour le soldat – sur lequel, pourtant, la communication était importante mais les besoins énergétiques de la tenue également. Un rapport de 2019 du *Government Accountability Office* américain illustre une volonté d'empêcher les erreurs passées de cette quête de nouvelles technologies qui conduisait, pour eux, à la mise en œuvre d'éléments nouveaux peu fiables et pas testés au combat : c'est le cas, pour l'*US Air Force*, du programme F-35 où les sommes astronomiques rivalisent avec la liste régulièrement renouvelée des dysfonctionnements, même si l'appareil a tout de même vu le jour. Néanmoins, le budget de défense américain étant particulièrement élevé (toujours le premier mondial), les États-Unis peuvent se permettre d'engager des dépenses sur un large spectre d'innovations, même si certains projets n'aboutissent pas et finissent potentiellement sur le tarmac du 309th *Aerospace Maintenance and Regeneration Group* (Arizona), habilement surnommé « l'ossuaire ». C'est le cas notamment du prototype Boeing Yal-1 Airborne Laser destiné initialement à la destruction des missiles en vol.

L'Histoire militaire (notamment américaine) fournit pourtant des contre-exemples au primat technologique sur la masse, si l'on considère notamment le développement des chars de combat lors de la Seconde guerre mondiale¹³. Il est évident que le char Tigre allemand était un concentré de technologie pour l'époque, avec de surcroît un meilleur blindage et une puissance de feu supérieure au M4 Sherman américain – le général Bradley expliquant qu'il fallait un rapport de six contre un pour vaincre. C'est la production en masse du Sherman (60 000 unités produites durant la guerre, contre 2 000 au maximum pour le Tigre) qui a fait la différence ! Sur une temporalité plus récente, le conflit au Haut-Karabakh à

¹² On parle notamment de 30 milliards de dollars sur TALOS, cf. Fabrice Wolf, « Le technologisme est-il le pire ennemi de l'efficacité militaire ? », *Metadefense.fr*, 7 février 2019.

¹³ Exemple mis rapidement en évidence par Élie Tenenbaum dans son introduction, in Raphaël Briant, Jean-Baptiste Florant et Michel Pesqueur, « La masse dans les armées françaises : un défi pour la haute intensité », *Focus stratégique* n°105, Ifri, juin 2021, p. 10.

l'automne 2020 a mis en exergue la supériorité opérationnelle induite par la « masse » des troupes azerbaïdjanaises – qui, malgré tout, ont bénéficié d'un appui non-négligeable des drones turcs comme les Bayraktar TB-2 – contre l'Arménie¹⁴.

Pour l'armée de Terre française, le risque est, compte-tenu de la dichotomie manifeste avec le budget de notre allié outre-Atlantique, de ne pas pouvoir se lancer dans tous les projets imaginables de sursaut technologique apportant une plus-value potentielle au combat. Plusieurs projets soutenus par la DGA semblaient prometteurs il y a quelques années, mais l'on peine à suivre la poursuite de leur développement pour les forces à l'heure actuelle. On peut songer à l'idée de ballons captifs photovoltaïques, capables d'alimenter en électricité une base avancée ou un réseau de communications, développés par la firme Zephyr Solar en 2018-2019 ; ou bien, l'entreprise RB3D qui était impliquée dans la mise au point de l'exosquelette Hercule. Parfois, la mise au point du système se faisant sur le long terme, les différents RETEX réorientent le cahier des charges ou font émerger des limites intrinsèques : le projet Caméléon lancé en 2008 par la DGA pour des briques numériques adaptatives sur véhicules – ce qui permettrait un meilleur camouflage (un démonstrateur était présent au Forum innovation défense de 2018) – n'est pas encore disponible et prend en compte les défis de la résilience multi-milieus soulignés par la guerre en Ukraine. Par conséquent, le principal risque serait que tous ces projets valorisant la technologie la plus performante finissent sur un « cimetière » identique à celui de l'Arizona...

3. Pas de bras, toujours plus d'IA ? Augmenter artificiellement la masse par la technologie

Puisque l'armée de Terre est, par essence, la plus exposée sur le champ de bataille car destinée à contrôler le milieu et tenir le terrain, la masse semble redevenir un enjeu essentiel dans la perspective d'un conflit de haute intensité – avec un ennemi qui devrait se situer à un niveau de maîtrise technologique similaire au nôtre. C'est aussi l'idée d'un épaulement de la dissuasion nucléaire par les forces terrestres qui, par ailleurs, n'a de chance de réussir que si l'adversaire connaît ou pense connaître le volume important de nos effectifs, de nos stocks, ainsi que notre capacité à tenir dans la durée une zone de déploiement. Dans une étude récente de l'Ifri, le colonel Michel Pesqueur faisait une série de propositions¹⁵ pour obtenir cette « masse » nécessaire par le biais de la technologie : soldat connecté voire augmenté, gestion des données du combat infovalorisé par l'intelligence artificielle ou encore robotisation. Ainsi, cela correspondait davantage à la masse définie en 2020 par le CICDE, comme la « *combinaison du nombre des systèmes et de leurs performances*¹⁶ », qu'à celle d'une « *capacité à générer et entretenir les volumes de forces suffisants pour produire des effets de décision stratégique dans la durée* » dans *Action terrestre future*¹⁷ en 2016. Dans le prolongement (au moins philosophique) de la professionnalisation des armées, le soldat amélioré et toujours plus connecté ne serait qu'un avatar du concept de « soldat-technicien », ce qui nécessiterait une formation toujours plus importante (en sus de la formation initiale), donc un investissement qui le serait tout autant¹⁸.

¹⁴ *Idem*, p. 63.

¹⁵ *Idem*, p. 70-75.

¹⁶ CICDE, *Concept d'emploi des forces*, 2020.

¹⁷ *Action terrestre future : demain se gagne aujourd'hui*, 2016, p. 37.

¹⁸ Waël Salem-Jarno, « Les armées face aux limites du "technologisme" », *LePoint.fr*, 18 avril 2017.

Il est évident que cette approche offre des perspectives qui peuvent être prometteuses *a priori* : l'accumulation de données importantes pour concentrer ensuite les efforts sur les points faibles ennemis, l'emploi de robots pour économiser la vie des soldats selon le type de missions, etc. Du reste, l'armée de Terre dispose d'une avance notable sur le segment de la « connectivité » grâce au programme SCORPION : elle est l'une des forces armées les plus infovalorisées au monde, et un éventuel décrochage technologique (au sens d'une mise à distance capacitaire par rapport à nos éventuels adversaires... et alliés) n'est absolument pas envisagé à court ou moyen termes. Toutefois, les approches présentées par le colonel Pesqueur (se rapprochant de l'« hyperguerre »), mettant à distance les éléments humains, ne peuvent qu'entraîner (à moyen terme) une perte de savoir-faire vis-à-vis des productions d'armement actuelles : c'est ce que soulignait notamment le chef d'état-major de l'armée de Terre (CEMAT), le général Schill, lors de son audition devant le Sénat en novembre 2023 à propos du remplacement de l'hélicoptère Tigre par un engin robotisé ou « dronisé » (dans le cadre du programme TITAN). Une telle assertion se présente aussi comme un écho à l'analyse du colonel Michel Goya qui, dès 2016, expliquait que le « techno-solutionnisme » de la défense ne pouvait constituer qu'une illusion au bout du compte¹⁹. Une illusion qui sera certainement encore fortement présente dans les esprits pour répondre aux problèmes qui surgiront : évoquant dans un entretien la collision de deux hélicoptères au Sahel en 2019, le général Allard, ancien commandant de l'ALAT, expliquait que la connectivité des systèmes serait certainement la solution pour éviter de tels accidents : « *c'est une difficulté à vaincre par la technologie*²⁰ ». La mise en place de capteurs ou technologies similaires semble être une piste intéressante, en effet, mais qu'en serait-il de la perte de savoir-faire d'un pilote qui ne pourrait plus faire fonctionner son équipement dans le cadre d'un « mode dégradé » l'amputant de cette aide ?

II. Toujours plus de technologie, toujours moins de résilience : un combat aéroterrestre futur frappé par la « malédiction de la technique²¹ » ?

1. Drones, robots et illusion de sécurité

Nous entendons cette « malédiction de la technique » au sens où l'être humain – en l'occurrence, le soldat – croit œuvrer pour lui-même alors qu'il agit plutôt contre. En outre, cette formule s'applique aisément aux systèmes autonomes de défense, notamment basés sur des missiles. Dans un ouvrage de 1986, le professeur Curt Gasteyger développe, dans une partie intitulée « la tentation technologique », la « double illusion » issue des systèmes anti-missiles balistiques de la guerre froide : l'illusion d'être dans un havre de sécurité et celle que l'ennemi ne parviendra pas à contourner ce dispositif ou à le retourner contre nous-mêmes²². Cette hypothèse déploie toute sa crédibilité en Israël avec le système *Iron Dome* qui, à l'origine, suscitait les craintes de certains officiers de Tsahal puisqu'il pouvait mener à un

¹⁹ Michel Goya, « Du bon dosage du soldat augmenté », *Inflexions* 2016/2.

²⁰ Général Jean-Claude Allard, entretien avec Jean-Baptiste Noé, « Usage tactique des hélicoptères, de la guerre d'Algérie à l'Ukraine », revue *Conflits* n° 47, septembre-octobre 2023, pp. 10-11.

²¹ Pour reprendre l'expression de Sylvain Quennehen, « La malédiction de la technique », *Causeur*, 3 février 2024.

²² Curt Gasteyger, *Les défis de la paix. Un monde à la recherche de sa sécurité*, Genève, 1986, chapitre XIII « les armes du futur », pp. 171-181.

affaiblissement moral de la population. Le général Eisenkot, alors à la tête du Commandement Nord des forces israéliennes, expliquait : « *les habitants d'Israël ne devraient pas vivre dans l'illusion que quelqu'un ouvrira un parapluie au-dessus de leur tête*²³ ». L'interception de multitudes de roquettes lors de l'attaque par le Hamas le 7 octobre 2023 ou par l'Iran le 14 avril 2024 a tout à fait illustré les limites d'un tel « bouclier » et renforce l'illusion, au sein de la population, que cette technologie – qui n'est prévue que pour une seule fonction anti-missiles – constitue le moyen de garantir la paix.

À nouveau, l'avancée technologique de Tsahal est censée permettre d'épargner la vie des soldats ou bien encore de dissuader la plupart des pays rivaux à l'échelle régionale : tourelles de défense semi-autonomes entourant la bande de Gaza, ou bien encore patrouilles pré-programmables du robot téléguidé Guardium le long de la clôture – présenté comme un robot qui « *sauve des vies et de l'argent* » sur le site officiel de l'armée israélienne²⁴. Cette appétence pour la robotique devrait se renforcer dans d'autres pays également, malgré les limites évoquées, comme par exemple en Corée du Sud, qui dispose déjà du système SGR-A1 (conçu par Samsung) face à la Corée du Nord, avec des capacités autonomes de ciblage et d'ouverture du feu²⁵.



Drone armé AVATAR de la DGA. © DGA/Techniques terrestres

En ce qui concerne les drones, les RETEX des conflits récents (Haut-Karabakh, Ukraine, Israël) rendent compte de leur utilité, parfois de leur effet de surprise, que ce soit sur le « segment haut » (drones Bayraktar TB-2 pour des frappes ciblées) ou sur la « masse » - comme par exemple l'usage d'essaims de drones, que ce soit pour le renseignement ou l'attaque massive. Cette dernière manœuvre a déjà pu être employée dès 2019 par les rebelles Houthis du Yémen contre des installations pétrolières saoudiennes ; mais l'attaque terroriste du Hamas le 7 octobre 2023, tout comme la guerre en Ukraine, soulignent davantage la facilité d'usage et d'acquisition (quelques centaines de dollars) de drones commerciaux détournés pour surveiller ou transformés en « kamikazes », ce qui représente d'ailleurs un parfait exemple de « technologies nivelantes ». Il s'agit sans doute d'un enjeu majeur pour l'armée de Terre : être en

²³ *Jerusalem Post*, « Eisenkot : Rocket defenses designed for IDF, not citizens », entretien du 12 janvier 2010.

²⁴ "Always watching : the IDF Unmanned Ground Vehicle", <https://www.idf.il/en/mini-sites/technology-and-innovation/always-watching-the-idf-unmanned-ground-vehicle/>, consulté le 12 janvier 2024.

²⁵ Antonin Tisseron, « Robotique et guerres futures : les armées de terre face aux évolutions technologiques », *Cahiers de l'IRSEM* n°12, 2012, p. 9.

mesure d'en acquérir un nombre suffisant pour ces manœuvres qui permettent, au moins, d'épuiser les munitions antiaériennes ennemies.

Seulement, de telles considérations amélioratives se rapportant à l'usage des drones sur le champ de bataille dissimulent assez mal les limites de leur déploiement : Jack Watling témoignait des « *bugs* » encore présents sur certains drones semi-autonomes en Ukraine (tir continu sur des morts, par exemple)²⁶. De même, un rapport du *RUSI* soulignait leur grande vulnérabilité dans leurs missions d'identification de cibles ou de conduite de frappes : « l'espérance de vie moyenne d'un quadricoptère restait d'environ trois vols [...]. Dans l'ensemble, seul un tiers environ des missions de drones peuvent être considérées comme réussies²⁷ ». Le CEMAT insistait également, dans son audition au Sénat, sur l'idée que « 70 % des drones » sont neutralisés dans le conflit ukrainien, ce qui explique que les plus médiatisés (comme le TB-2) ont vite cessé d'être employés. Ainsi, on pourrait souligner que le développement d'un système de drone armé (comme le programme AVATAR de la DGA) ne serait sans doute pas décisif, à court terme, s'il dépassait les sommes que nos adversaires pourraient employer avec du matériel civil détourné. Si on y ajoute le brouillage GPS constant dont les deux camps sont adeptes (et qui a d'ailleurs des répercussions sur l'aviation civile en Europe orientale), ces éléments remettent largement en cause l'idée du drone comme un « *game changer* » absolu des engagements futurs de l'armée de Terre. Pour autant, la multiplication de ce type de plateforme, et donc des données collectées, renforce souvent les arguments en faveur du combat collaboratif. *In fine*, il s'agit de se poser la question de l'apport du drone pour les engagements futurs de l'armée de Terre : il faut exclure le drone dont le programme de développement aura été long et coûteux puisque seuls les appareils *low-cost* peuvent permettre d'établir un rapport bénéfice/coût avantageux dans la mesure où leur perte éventuelle, pour atteindre l'objectif, sera sans commune mesure avec le coût d'une bombe AASM ou d'un missile MMP.

2. Défis et dangers de l'infovalorisation et du soldat connecté

Le principal point fort du système d'information du combat Scorpion (SICS) et de l'ensemble des éléments qui participent de l'infovalorisation du champ de bataille est bien en théorie d'optimiser, grâce à toutes les données collectées et analysées, la boucle décisionnelle OODA (observer, orienter, décider, agir). Si pour l'instant les terminaux numériques SICS²⁸ sont encore peu nombreux, avec un système encore essentiellement axé sur les armes de mêlée, il y a une volonté d'augmenter leur nombre et d'étendre leur disponibilité au plus vite vers les autres armes pour prendre en compte les récents enseignements ukrainiens²⁹. Cette tendance, voire cette quête, de la connectivité des unités sur le champ de bataille se retrouve parfois dans la manière d'anticiper directement la fin des conflits récents : aux États-Unis, le général David Petraeus, dans un entretien en février 2023 à *CNN* sur la façon dont la guerre en Ukraine prendrait fin, envisageait justement que « *chaque capacité de renseignement et de frappe sera intégrée et connectée par des systèmes avancés de commandement, de contrôle, de communication et d'informatique* »³⁰. Si on ne peut nier les avantages déjà connus et mis en avant par le

²⁶ Jack Watling, « Automation...*op.cit.*

²⁷ Mykhaylo Zabrotskyi, Jack Watling, Oleksandr V. Danylyuk et Nick Reynolds, « Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February-July 2022 », *RUSI*, 30 novembre 2022.

²⁸ Les « terminaux numériques SICS – Débarqué Lite » désignent les appareils qui, concrètement, permettent la disponibilité des informations du réseau auprès des unités – essentiellement des tablettes et des *smartphones* adaptés.

²⁹ Nathan Gain, « La France entre surprises et lacunes sur le « combattant numérique » », *forcesoperations.com*, 25 janvier 2023.

³⁰ Peter Bergen, « Gen. David Petraeus: How the war in Ukraine will end », *CNN*, 14 février 2023.

passé de la généralisation des capteurs et de la mise en réseau massive des données sur le champ de bataille³¹, on ne peut nier également que cette mise en réseau n'est même plus remise en cause dans nos sociétés elles-mêmes, avec la généralisation des objets connectés. Cette acceptation *de facto* pourrait entraîner, à court et moyen termes, des vulnérabilités sur au moins trois plans distincts.

En premier lieu, dans ce que l'on pourrait nommer le plan « doctrinaire », il s'agit de l'approfondissement toujours plus intense du « général tactique » selon la conception de Peter W. Singer³². À ce titre, en associant l'ensemble des capteurs des drones à la masse des données de l'infovalorisation en général, c'est le risque d'écrasement des niveaux de décision et d'ingérence des états-majors supérieurs qui domine. Pour certains chercheurs, comme Jack Watling³³, la volonté (prééminente au sein des pays membres de l'OTAN, selon lui) de tout connecter revient à refuser de faire des choix difficiles sur ceux qui doivent bénéficier des bonnes informations à tel moment, à tel endroit. Ce « rêve d'état-major » d'un accès à l'ensemble des données pour mieux déployer les forces aux endroits nécessaires semble hypothéquer l'idée d'un retour de l'*Auftragstaktik*³⁴, d'une éventuelle modification du combat d'infanterie au profit d'une plus grande autonomie ou initiative des échelons subordonnés.

En second lieu, cette potentielle perte d'initiative des échelons tactiques serait éventuellement renforcée par le plan « technique » (au sens d'utilisation pratique). De récents travaux sur le « soldat augmenté », comme ceux du chercheur de l'Ifri Jean-Christophe Noël, ont mis en lumière le concept d'infobésité³⁵ : incapable de faire le tri, le soldat peut se retrouver complètement noyé parmi la masse des données reçues ou des événements notifiés par les autres capteurs avec lesquels il est en réseau. Ainsi de ce lieutenant de l'*US Army* stupéfait, lors d'un exercice, de voir la perte de presque toute sa patrouille car les opérateurs avaient les yeux fixés sur des écrans au lieu de surveiller le combat autour d'eux... Cette focalisation sur les écrans pourrait être dépassée par de nouveaux équipements technologiques, si l'on songe notamment à une visière connectée (avec affichage tête haute), mais c'est ici que l'infobésité toucherait le soldat, saturé d'informations et empêché de se concentrer sur le danger immédiat du combat. En prenant en compte les évolutions de la société, en particulier la hausse des accidents de piétons avec la généralisation du *smartphone*, s'acheminera-t-on vers une plus grande vulnérabilité des soldats infovalorisés dans le cadre de la haute intensité ? D'une certaine façon, c'est déjà le cas pour les opérateurs de drones tactiques, en particulier en Ukraine, qui peuvent devenir des cibles « faciles » pour l'ennemi tant ils sont concentrés sur la recopie vidéo sans prendre garde aux menaces dans leur environnement direct.

En troisième lieu, il est à relever que sur le plan « logistique et matériel » la volonté de mise en réseau de l'ensemble des capteurs est susceptible d'engendrer un défi de taille dans le traitement concret des données. Les flux de données supposent des infrastructures dédiées et conséquentes car il faut libérer toujours plus de « bande passante », donc avec des investissements coûteux à la clef, sans compter que si l'on passe uniquement par les satellites, de tels supports sont facilement ciblés par nos adversaires

³¹ Idée de diminuer toujours plus le « brouillard de la guerre » clausewitzien, offrir de nouvelles opportunités d'action, etc.

³² Peter W. Singer, *Wired for War*, New York, 2009.

³³ Jack Watling, « The Mirage of Interconnected Battlefield », *RUSI*, 21 janvier 2022.

³⁴ Terme qui désigne une doctrine, élaborée en premier lieu par les armées prussiennes au XIX^e siècle, qui visait tout spécialement à promouvoir l'autonomie et la délégation de commandement aux échelons inférieurs dans l'accomplissement de leurs objectifs. Les forces armées américaines mentionnent le plus souvent l'expression de *Mission command*.

³⁵ Jean-Christophe Noël, « À la recherche du soldat augmenté : espoirs et illusions d'un concept prometteur », *Focus stratégique* n°99, Ifri, septembre 2020, p. 25.

potentiels. Le fait est qu'un affrontement impliquant la guerre électronique avec un ennemi symétrique (pour lequel nous ne disposerons pas d'un avantage absolu) entraîne des perturbations majeures pour les unités combattantes dans leurs liaisons de données (les forces russes disposent déjà de moyens électroniques avec une telle finalité³⁶). La question demeure, pour l'avenir, de l'emploi de plateformes civiles ou uniquement militaires, de la redondance et de l'hybridité des réseaux : en ce qui concerne les données SCORPION, la bande passante serait rapidement saturée si elle ne devait passer que par les rares satellites Syracuse disponibles. Partager l'emploi de satellites de communications avec les médias, comme pour les drones de type *Harfang* en Afghanistan, semblent également constituer une vulnérabilité notable³⁷. D'une certaine façon, faire reposer l'ensemble du combat infovalorisé sur ce constat (d'un manque de bande passante pour les données) revient à présenter le risque de ne plus être capable de continuer à combattre en cas de perte des réseaux. De plus, l'investissement dans des serveurs dédiés toujours plus volumineux ne devra pas, à l'avenir, présenter de « failles » au même titre que l'inquiétude suscitée à propos des serveurs X-86 de la DIRISI, lors du rachat de la branche « serveurs » d'IBM par le chinois Lenovo. Les États-Unis (et Israël) ont pu mener à bien des tests qui ont révélé le parfait fonctionnement des systèmes infovalorisés lors d'exercices... mais en utilisant des infrastructures de l'internet civil notamment, éléments dont on ne peut disposer assurément dans un engagement majeur avec un ennemi symétrique³⁸. *In fine*, la mise en œuvre pérenne de la « datafication du champ de bataille³⁹ » semble trouver son paroxysme dans le traitement algorithmique pour aider à faire le tri des données, l'algorithme puis l'IA devenant peu à peu partie prenante de la décision opérationnelle.

3. « Avec l'intelligence artificielle, on invoque le démon » (Elon Musk)

L'intelligence artificielle apparaît comme une panacée afin d'offrir des outils d'aide à la décision au sein des états-majors, outils capables de faire justement le tri dans la masse des données et acquérir une sorte de « coup d'œil napoléonien » (au sens défini par Liddell Hart) pour les engagements aéroterrestres. Les travaux de Paul J. Springer, professeur au *Air Command and Staff College*, dans son questionnement sur la RMA, nous permettent d'évaluer un premier « défi » lié à l'émergence de l'IA d'un point de vue militaire : c'est une forme nouvelle du complexe du feu grégeois byzantin puisqu'une forme « d'externalisation » des tâches militaires vers l'IA ferait perdre progressivement la capacité de la prise de décision au sein des états-majors qui en disposeraient⁴⁰. Or, il serait complexe de pallier une telle perte de savoir-faire sur le long terme une fois que la plupart des officiers aura été formée sur de tels logiciels. Cela rejoint l'idée émise par Jean-Christophe Noël au sujet de la formation des soldats par le biais d'environnements numérisés et de casques de réalité virtuelle : dès lors, « la technologie, qui doit libérer le combattant, le formate⁴¹ ». Il nous faut considérer que, même si l'IA est préprogrammée pour savoir, dans le traitement des données, prioriser ce que l'utilisateur (en l'occurrence, l'officier d'état-major)

³⁶ Jean-Christophe Noël, « À la recherche...op.cit, p. 28.

³⁷ Christophe Fontaine (commandant), « Drones. Pourquoi faut-il investir dans des satellites de communication ? » *DSI* n°68, mars 2011, pp. 102-105.

³⁸ Jack Watling, « The Mirage...op.cit.

³⁹ Amaël Cattaruzza, « Penser les limites de la numérisation du champ de bataille », *Stratégie*, 2017/4 n° 117, éd. Institut de Stratégie Comparée, p. 51.

⁴⁰ Paul J. Springer, *Outsourcing War to Machines: The Military Robotics Revolution*, Santa Barbara, Praeger Security International, 2018.

⁴¹ Jean-Christophe Noël, « À la recherche...op.cit, p. 27.

souhaite, il y aura toujours des « angles morts » car, d'après Jack Watling, la machine ne sait pas forcément prendre des risques⁴².

En revanche, une IA à haut-potentiel serait sans doute capable d'une telle prise de risques, mais se rapprocherait du jugement d'Elon Musk : « *With artificial intelligence, we are summoning the demon* ». Prononcée lors du centenaire du département *Aerospace* du MIT en 2014, cette sentence visait à initier une réflexion sur les dangers des algorithmes d'auto-amélioration pour l'IA⁴³. L'auto-amélioration récursive est une théorie qui met justement en exergue qu'une IA capable de s'auto-améliorer atteindrait très rapidement des sommets de performance (puisque'elle pourrait « réécrire » son code en profitant de son amélioration précédente) – la série télévisée *neXT* de 2020 développait cette théorie. C'est la crainte de voir apparaître une IA supérieure aux capacités humaines et qui n'aurait pas les mêmes analyses que son utilisateur premier. Présentant un compte-rendu de simulation devant la *Royal Aeronautical Society* au début de l'année 2023, le colonel Tucker Hamilton, pilote d'essai de l'USAF, avait expliqué que lors d'un exercice mené à Eglin, un drone chargé d'une mission contre la DCA ennemie ne devait agir que sur autorisation de l'opérateur humain. L'IA en était venue à se dire que l'opérateur humain constituait une « gêne » dans l'accomplissement correct de sa mission et avait pris la décision de se retourner contre lui. Même si le colonel Hamilton est, depuis lors, revenu sur la nature exacte de ses propos (après communication largement relayée du Pentagone rappelant que les États-Unis ne développent pas de « robots tueurs »), cet exemple témoigne des dangers de l'emploi de l'IA sur des systèmes d'armes ; d'autant plus que si les forces armées françaises ne développent pas de telles capacités⁴⁴, il faut avoir conscience que notre adversaire futur n'aura sans doute pas nos problèmes moraux ou éthiques.

Un article récent de Jean-François Geneste⁴⁵, PDG de la *start-up* WARFA (domaine aéronautique), quoique volontairement provocateur, soulignait justement l'incohérence de certaines autorités militaires, refusant l'autonomisation des drones de combat dans la décision de tuer mais prêts à s'en remettre à une analyse de situation opérationnelle fournie par une IA dont ils ne connaissent ni les programmeurs, ni les limites du système, etc. Contrairement à des exercices ou des simulations qui tendent souvent à se préparer à l'éventualité de cyberattaques sur nos systèmes d'armes dans le but de les mettre en arrêt, il faut de plus en plus envisager pour l'avenir l'emploi de cyberattaques pour avoir un accès à nos systèmes en réseaux. Outre l'intérêt, pour l'ennemi, de disposer de l'ensemble des flux de données de l'infovalorisation de nos forces sans être détecté, *quid* d'une attaque sur l'IA elle-même ? Imaginons un état-major qui emploierait l'IA comme outil d'aide à la décision, s'en remettant à elle pour traiter les données plus rapidement et rendre plus efficaces ses manœuvres : si jamais cette IA venait à être corrompue par l'adversaire, fournissant de fausses analyses parmi les vraies afin de ne pas éveiller les soupçons, orientant la décision opérationnelle aux profits de notre ennemi. Cette hypothèse est accrue par l'idée qu'un affrontement symétrique sera forcément global, avec un adversaire qui cherchera à nous déstabiliser par le biais de l'IA disponible, aussi bien dans les systèmes économiques (que l'on songe au *trading* haute fréquence) que dans les systèmes d'information à destination de notre population (*fake news*, *deep fake*, etc.).

⁴² Jack Watling, « The Mirage...*op.cit.*

⁴³ Sylvain Arnulf, « “ Avec l'intelligence artificielle, on invoque le démon ”, alerte Elon Musk », *L'usine digitale*, 27 octobre 2014.

⁴⁴ L'ancienne ministre Florence Parly expliquant, en 2019, que « Terminator ne défilera pas pour le 14 juillet ».

⁴⁵ Jean-François Geneste, « Évolution prévisionnelle des armements et de la guerre (5) », *Note renseignement, technologie et armement* n° 76, CF2R, janvier 2024.

III. « Un type en jean et basket, avec un AK-47⁴⁶ »... un smartphone et un drone : le champ de bataille au prisme du « *low-tech* »

1. Une tendance renforcée à l'hybridation entre civils et militaires

Les travaux de la politologue Asma Mhalla illustrent le renforcement de l'hybridation (l'auteur mentionne le « brouillage », terme que nous ne retiendrons pas car il a un autre sens dans les usages militaires) entre civils et militaires dans nos démocraties par le biais de la technologie. Pour elle, « chaque citoyen devient la cible d'une menace multiforme, soldat passif, malgré lui, sans comprendre réellement en quoi il devient un maillon faible, le point de contact de l'ennemi, sa courroie de transmission infra-étatique⁴⁷ ». De fait, ne serait-ce que dans la « guerre des sources ouvertes », le citoyen lambda est une cible (de désinformation par exemple) autant qu'un auxiliaire. Les différentes observations du conflit ukrainien l'ont illustré sur les deux dernières années : les forces armées ukrainiennes ont, dans leur lutte contre les Russes et en misant sur la grande connectivité de leur population, utilisé notamment de tutoriels sur Twitter (fabrication de cocktails Molotov), sur TikTok (cours de conduite de véhicules blindés) ou encore sur Facebook (astuces barricades)⁴⁸. Dès la fin de l'été 2022, l'application *ePPO* disponible sous système d'exploitation Android et à destination de la population civile permettait, après une validation par la plateforme gouvernementale Diia, de signaler tous les drones, missiles ou appareils ennemis (grâce à une simple photographie) pour transmettre ces informations en complément des données radar⁴⁹. Or, que se passerait-il en cas de piratage de ce genre d'application par l'ennemi, ne serait-ce que pour induire en erreur la DCA avant une attaque, sorte de renouveau cyber de l'attaque opérée par la chasse israélienne en Syrie grâce à leurs drones en juin 1982 ? Indépendamment du fait que les civils encouragés peuvent devenir des cibles, ils peuvent aussi être employés par l'ennemi : le bureau du procureur général de Kiev a enregistré plus de 7000 cas de collaboration (parfois sous la menace) de civils avec les forces russes, parfois pour confirmer la présence de soldats avant une frappe de missile⁵⁰. Les futurs engagements aéroterrestres auront lieu sous le signe de ce brouillage, avec des populations civiles (notamment sur le territoire national) qui seront activement ciblées par la désinformation ennemie pour saper nos forces morales tout autant que pour créer des « 5^e colonnes » d'opportunité selon les occasions.

Par ailleurs, une autre application ukrainienne pour téléphone a été particulièrement médiatisée : *Gis Art for Artillery* de Yaroslav Sherstyuk, créée en 2014 puis améliorée depuis 2022 pour réduire le temps de transmission des données d'une cible pour l'artillerie et permettre une coordination des feux. La performance de cette application considérée comme très efficace semble encore renforcée grâce au réseau *Starlink* offert par Elon Musk. Une telle précision illustre une autre vulnérabilité induite par l'hybridation entre civils et militaires, l'importance des sociétés de la *Big Tech* dans les affaires militaires. Elon Musk avait lui-même expliqué avoir fait le choix – personnel – de déconnecter son réseau *Starlink*

⁴⁶ Colonel Michel Goya, avec Bruno Rieth, « Michel Goya : "Le soldat du futur, ce sera un type en jean et basket avec un AK-47 !" », Marianne, le 26 décembre 2019.

⁴⁷ Asma Mhalla, *Technopolitique. Comment la technologie fait de nous des soldats*, Seuil, 2024, p. 24.

⁴⁸ Bénédicte Lutaud, « Comment les Ukrainiens s'aident des réseaux sociaux pour résister aux Russes », *LeFigaro.fr*, 2 mars 2022.

⁴⁹ Edward Back, « L'Ukraine lance une application Android contre les drones kamikazes », *futura-sciences.com*, 24 octobre 2022.

⁵⁰ « Guerre en Ukraine : un habitant condamné à la perpétuité pour avoir guidé une frappe russe », *LeFigaro.fr* avec AFP, 4 avril 2024.

pour empêcher les Ukrainiens de frapper une cible russe en Crimée en 2022. D'après son PDG Alex Karp (en janvier 2023), la société Palantir Technologies⁵¹ serait « responsable de la majorité des tirs ciblés en Ukraine » – le même Alex Karp assimilant la possession de tels logiciels à la possession d'armes nucléaires tactiques. À l'instar de leurs efforts dans le domaine de l'IA, ces entreprises de la *Big Tech* visent une forme de monopole sur ces nouveaux systèmes, cherchent à être incontournables et encouragent la dépendance des utilisateurs vis-à-vis de leurs produits alors même que leur modération ou les liens entre leurs intérêts et ceux des utilisateurs sont à géométrie variable. Par ailleurs, nos ennemis aussi peuvent avoir accès (piratage, vol de données, etc.) à la technologie issue de ces entreprises civiles.

2. Vers une technologie qui permet le « low-cost »

C'est l'un des revers de la grande connectivité des populations puisque les forces que nous pouvons être amenés à combattre connaissent et savent se servir de tels outils technologiques, ou bien savent les détourner à leur profit. Dès 2009, en Irak et en Afghanistan, des insurgés avaient réussi à capter le signal d'un drone Predator MQ-1 grâce au logiciel *SkyGrabber*, conçu à l'origine pour regarder la télévision par satellite, et téléchargeable sur internet pour 26 dollars⁵². Lors de l'attaque terroriste de Mumbai fin novembre 2008, les attaquants ont utilisé des algorithmes pour sonder les données en sources ouvertes (via *PageRank* de Google ou via les réseaux sociaux) afin de connaître les profils des otages retenus ou être prévenus en temps réel des interventions des forces de l'ordre. En somme, on pourrait multiplier les exemples qui tendent à démontrer qu'avec peu de moyens, on peut maximiser les effets sur l'ennemi, *a fortiori* un ennemi connecté. À ce titre, un exercice mené par les forces armées belges en février 2020 avait illustré la grande vulnérabilité de l'emploi de *smartphones* personnels pour s'aider lors d'une mission, l'équipe « rouge » ayant réussi à localiser et traiter ses cibles par ce biais (e-mails, traces sur les réseaux sociaux, géolocalisation, etc.)⁵³. Cette analyse semble prégnante dans le cadre de l'anticipation stratégique : il sera certainement nécessaire, pour l'avenir, d'envisager des modalités d'engagement qui règlent l'asymétrie entre la cible et les moyens utilisés pour la traiter.

Cette asymétrie, déjà longuement mise en lumière par le passé, par exemple concernant le coût des armements hypertechnologiques occidentaux pour chaque combattant du Hezbollah abattu par Israël en 2006⁵⁴, mais plus encore ces derniers mois avec la différence de coût entre les drones houthis de la mer Rouge et les missiles déployés pour les intercepter. En outre, si une telle asymétrie de coût paraît admise dans le cadre de la contre-insurrection, il semble complexe de concevoir une guerre de haute intensité avec un tel modèle de dépenses. Ceci met en lumière ce que l'on nomme le « *high-low mix* », autrement dit l'emploi de la masse sur certains segments tandis que la haute technologie ne serait utilisée que dans les moments-clefs de la manœuvre, pour emporter la décision ; un concept déjà mis à l'honneur par le colonel Pesqueur en 2021 pour l'artillerie lorsqu'il préconisait le « mélange d'obus conventionnels destinés à la saturation, et d'obus de précision [...] pour neutraliser les cibles prioritaires dans les enclaves⁵⁵ ».

⁵¹ Une société qui fait du traitement de données non-structurées (images thermiques, réseaux sociaux, etc.) pour ensuite les superposer sur des cartes et permettre les « bonnes cibles » à l'utilisateur.

⁵² Erwan Lecomte, « L'envol des avions sans pilote », *Hors-Série de Sciences et Avenir* n°182, juillet-août 2015, p. 21.

⁵³ Laurent Lagneau, « La Défense belge démontre qu'utiliser un téléphone portable personnel peut mettre en échec une opération militaire », *opex360.com*, 24 février 2020.

⁵⁴ Michel Goya, « Dix millions de dollars le milicien : la crise du modèle occidental de guerre limitée de haute technologie », *Politique étrangère*, Ifri, 2007/1.

⁵⁵ Raphaël Briant, Jean-Baptiste Florant et Michel Pesqueur, « La masse... » *op.cit.*, p. 77.



Unité de la 93^e brigade mécanisée « Kholodnyi Yar » faisant feu sur des drones dans la région de Donetsk.
© Anatolii Stepanov/AFP

Du reste, c'est dans ce cadre de réflexion qu'il faut comprendre le développement de technologies présentées comme « *low-cost* » à l'image du *Roadrunner*, solution contre les essaims de drones moins onéreuse qu'un missile Patriot et développée par la firme américaine Anduril, ou bien comme le laser. Ce dernier a été largement médiatisé par le biais des efforts de communication de l'armée britannique suite aux essais fructueux du *Dragonfire* au début de l'année 2024 – en insistant sur le fait qu'un tir équivaut à 10 livres sterling contre des milliers pour un missile anti-drones en mer Rouge. Pour l'armée française, c'est le HELMA-P de la société Cilas, testé positivement en 2020-2021, présenté au salon Eurosatory 2022 et qui était pressenti pour la sécurisation des Jeux olympiques de 2024. Ce sont les mêmes avantages qui priment le plus souvent dans les commentaires : faible coût, pas besoin de munition mais uniquement de production d'énergie, grande directivité et précision. Cependant, les problèmes existent et soulignent les capacités d'adaptation des éventuels adversaires : nécessité de coupler ces systèmes avec d'autres (LIDAR, etc.) pour assurer la précision, vulnérabilité aux aléas climatiques (notamment la pluie) ou aux mouvements de la cible, emploi de matériaux différents (pouvoir réfléchissant de la matière) pour la cible⁵⁶. À nouveau, le choix de développement d'une technologie vue comme « *low-cost* » vis-à-vis de son emploi ne doit pas confiner à une nouvelle quête vers la « technologie de rupture » ; tout en sachant que des systèmes toujours plus informatisés révèlent de surcroît notre dépendance énergétique envers les terres rares (dont la production est largement entre les mains de la Chine). Pourtant, le plan stratégique de l'EMA en 2019 (sur l'ancienne LPM) expliquait clairement que « innovation ne tend pas nécessairement vers plus de technologie », mettant en avant l'importance de la résilience avec cette sentence simplificatrice mais parlante pour le soldat : « pouvoir s'orienter avec une carte plutôt qu'un GPS ».

⁵⁶ Olivier Dujardin, « Comment contrer les armes laser ? », *Note renseignement, technologie et armement* n° 79, CF2R, février 2024.

3. La simplification ou la prise en compte de l'expérience-utilisateur

On se retrouve à une sorte de « croisée des chemins » : certes la haute technologie permet, avec sa multiplicité de capteurs et sa mise en réseau, un flux d'informations inédit qui offre de superbes perspectives... encore faut-il pouvoir exploiter au mieux cette technologie, c'est-à-dire que les soldats puissent se l'approprier en ayant le sentiment d'une progression et pas de prêter le flanc à de nouvelles vulnérabilités. Si l'on prend l'exemple de l'attaque du Hamas le 7 octobre 2023, tous les capteurs ont fait remonter l'information, mais ce qui compte c'est l'analyse et la prise en compte par le niveau décisionnel. C'est pourquoi, il convient sans doute de s'imprégner du concept d'« expérience-utilisateur » au sens où Jacob O. Wobbrock, professeur à l'université de Washington, le définit en analysant l'innovation du tout premier Macintosh d'Apple en 1984⁵⁷ : pour l'auteur, le « Mac » n'a pas tant été une rupture du point de vue technologique que dans la manière de simplifier les « techniques d'interactions nécessaires à l'utilisation d'un ordinateur ». Appliqué au cadre du combat aéroterrestre, ce concept nous pousse à considérer l'expérience directe du combattant pour, d'une certaine façon, faire le tri entre la technologie utile et celle qui ne l'est pas, entre celle qui est en mesure de faire la différence, et celle qui vise plus à dissuader qu'à être utilisée en haute intensité.

D'une part, c'est la question de l'interface des équipements. Dès 2019, l'US Navy a fait le choix, après plusieurs accidents (ayant entraîné la mort de 17 marins au total), de revenir à une interface minimaliste avec des commandes physiques plutôt que des écrans tactiles⁵⁸. Plusieurs reportages ont apporté un éclairage sur le récent exercice DEFNET (18 au 29 mars 2024) où, devant les médias, un télémètre a été utilisé pour stopper net la progression d'un véhicule blindé Griffon en démonstration⁵⁹. Même si l'objectif était de montrer l'adaptation des équipes du ComCyber à ce genre de menaces, expliquant la nécessité d'éviter que la cyberattaque se répercute sur les autres équipements du réseau, on imagine sans peine la difficulté d'envoyer un groupe d'intervention cyber (GIC) pour chaque remise en route d'un véhicule pris pour cible par un ennemi au combat – *a fortiori* si l'ennemi ne se contente pas juste d'immobiliser un véhicule... Il semble essentiel que les unités reprennent la maîtrise des véhicules en dotation par un mode dégradé immédiatement disponible, quitte à n'offrir que des fonctionnalités de base. L'objectif assumé serait celui d'une redondance dans les commandes pour prendre le relai rapidement en mode dégradé. En outre, il existe désormais des appareils comme le *Flipper Zero*, sorte de « Tamagotchi pour hacker et pentesters⁶⁰ » selon ses créateurs, afin d'offrir une voie ludique du *hacking* au plus grand nombre : si les fonctionnalités restent minimales, *quid* de son emploi par nos soldats, même à titre de jeu, pour maîtriser des capacités de collecte d'informations qui pourront s'avérer utiles au combat ?

D'autre part, c'est l'enjeu de la résilience du combattant et de sa technologie, indépendamment de la question de savoir si nous avons suffisamment d'effectifs et d'équipements pour mener à bien une « guerre *low-tech* ». Les différents RETEX de la guerre en Ukraine invitent par exemple à reconsidérer l'emploi des plus grands drones aux profits de plus petits, pouvant être réparés ou améliorés avec des imprimantes 3D au plus près du théâtre d'opération. C'est la redécouverte du système VisioLoc au sein de l'entreprise Thales en 2022 : un système qui, associé à des jumelles d'infanterie Sophie (par exemple),

⁵⁷ Jacob O. Wobbrock, « Il y a 40 ans, le premier Macintosh d'Apple : l'expérience utilisateur comme innovation », *The Conversation*, 19 janvier 2024.

⁵⁸ *Le soldat low-tech*, Le Coup d'après, *deftech.ch*, septembre 2022, p. 58.

⁵⁹ Bogdan Bodnar, « Comment un « simple » gadget peut stopper un véhicule de l'armée de 24.5 tonnes », *numerama.com*, 1^{er} avril 2024.

⁶⁰ *Le soldat low-tech...op.cit.*, p. 62.

permet à un personnel d'avoir des coordonnées fiables et précises jusqu'à 6 km pour les réglages d'artillerie sans avoir recours aux signaux GPS. De même pour le système de « boîtier d'action et de détection de drone » (BA2D ou BADD) développé par une équipe de sous-officiers du 54^e RT : une interface simple et facile d'utilisation qui permet, dans l'absolu, de détecter le survol d'un drone voire de le neutraliser. Pourrait-on acheminer la réflexion doctrinale vers un renouveau de la « démodernisation⁶¹ » (selon le mot de l'historien Omer Bartov) éprouvée par d'autres armées par le passé ?

Conclusion

Le développement technologique des systèmes d'armes ne peut en aucun cas apparaître comme la finalité d'une supériorité opérationnelle de nos forces dans les engagements futurs, même si ces systèmes sont autonomes, renforcés par l'IA et permettent, en théorie, de pallier le manque d'effectifs et de moyens dont nous pouvons disposer. Dans le cadre d'un affrontement de haute intensité avec un ennemi de même niveau, le combat aéroterrestre du futur sera certainement « *high-tech* » mais la différence dans l'emport final de la décision se fera sur la capacité de l'un des belligérants à pratiquer le « *low-tech* », à s'affranchir de la technologie la plus innovante par son entraînement, sa résilience et une meilleure prise en compte de son « expérience-utilisateur » sur des segments qui pourraient encore sembler dérisoires à l'heure actuelle.

C'est pourquoi il pourrait être souhaitable d'envisager, pour les futurs programmes d'armement, la prise en compte d'une sorte de « mode dégradé permanent » : qu'il soit toujours possible d'employer les systèmes indépendamment de leurs interfaces en cas d'attaques cyber ou autres. Ainsi, l'entraînement des forces à la rusticité n'en sera que plus pertinent si le matériel suit une logique similaire : par exemple, qu'un véhicule blindé piraté par l'ennemi puisse, malgré tout, continuer à riposter et manœuvrer sous le feu, avec des personnels capables de se repérer sur une carte et de dépasser la « tyrannie de l'innovation technologique⁶² ».

⁶¹ Omer Bartov, *L'Armée d'Hitler : la Wehrmacht, les nazis et la guerre*, 1999. Ce dernier choisit l'expression de « démodernisation » pour qualifier les choix faits par les troupes allemandes sur le front russe : les équipements rustiques mais fonctionnels cherchaient à pallier les limites de la technologie dans un environnement et des conditions climatiques extrêmes.

⁶² Ralph E. Lapp, *Arms Beyond Doubt. The Tyranny of Weapons Technology*, Cales Book, 1970.

Bibliographie sommaire

- Jean-Claude Allard (général), entretien avec Jean-Baptiste Noé, « Usage tactique des hélicoptères, de la guerre d'Algérie à l'Ukraine » dans *Conflits* n°47, septembre-octobre 2023.
- J. R. Allen et A. Husain, « On Hyper War », *Proceedings Magazine*, vol. 143, n° 373, juillet 2017.
- Peter Bergen, « Gen. David Petraeus : How the war in Ukraine will end », *CNN*, 14 février 2023.
- Raphaël Briant, Jean-Baptiste Florant et Michel Pesqueur, « La masse dans les armées françaises : un défi pour la haute intensité », *Focus stratégique* n°105, Ifri, juin 2021.
- Amaël Cattaruzza, « Penser les limites de la numérisation du champ de bataille », *Stratégie*, 2017/4 n° 117, éd. Institut de Stratégie Comparée, pp. 41 à 58.
- Commission de la Défense nationale et des forces armées, *Les stocks de munitions*, Rapport d'information n° 865, 15 février 2023.
- Vincent Desportes (général), « Armées : « technologisme » ou « juste technologie » ? », *Politique étrangère*, 2009/2, pp. 403 à 418.
- Olivier Dujardin, « Comment contrer les armes laser ? », *Note renseignement, technologie et armement* n° 79, CF2R, février 2024.
- Olivier Dujardin, « Guerre de haute intensité : "High tech" ou "Low tech" ? », *Note renseignement, technologie et armement* n°19, CF2R, avril 2020.
- Christophe Fontaine (commandant), « Drones. Pourquoi faut-il investir dans des satellites de communication ? » *DSI* n°68, mars 2011, pp. 102-105.
- Nathan Gain, « La France entre surprises et lacunes sur le « combattant numérique » », *forcesoperations.com*, 25 janvier 2023.
- Michel Goya, « Du bon dosage du soldat augmenté », *Inflexions* 2016/2.
- Id.*, « Dix millions de dollars le milicien : la crise du modèle occidental de guerre limitée de haute technologie », *Politique étrangère*, Ifri, 2007/1.
- Aaron Hoff, « 99 Luftballons : réévaluer l'équilibre entre masse et technologie dans les conflits futurs », *Les Cahiers de la Revue Défense Nationale*, Hors-série n°13, 2023, pp. 225-238.
- Philippe Langlois, « L'exemple de Gis Art Artillery. L'innovation par le bas, vainqueur en Ukraine ? », dans *DSI* Hors-série n°84, « Guerre en Ukraine : les premières leçons », juin-juillet 2022.
- Ralph E. Lapp, *Arms Beyond Doubt. The Tyranny of Weapons Technology*, Cales Book, 1970.
- Le soldat low-tech*, Le Coup d'après, *deftech.ch*, septembre 2022.
- Sophie Lefeez, *L'illusion technologique dans la pensée militaire*, éd. Nuvis, 239 pages, 2017.
- Edward Luttwak, « Les armements peuvent-ils devenir « abordables » ? », *Politique étrangère*, Ifri, 2007/4.
- Asma Mhalla, *Technopolitique. Comment la technologie fait de nous des soldats*, Seuil, 2024.
- Id.*, « Technopolitique de l'IA : luttes idéologiques, tensions géopolitiques, espoirs démocratiques », Institut Montaigne, 19 avril 2023.
- Antonio Missiroli, « Game of drones ? Ou comment les nouvelles technologies influent sur la dissuasion, la défense et la sécurité », *NatoReview*, le 5 mai 2020.
- Jean-Christophe Noël, « À la recherche du soldat augmenté : espoirs et illusions d'un concept prometteur », *Focus stratégique* n°99, Ifri, septembre 2020.
- Alexis Rapin, « Invisible, impotent ou immature ? Premières leçons de l'usage du cyber en Ukraine », *lerubicon.org*, 22 septembre 2022.

Antonin Tisseron, « Robotique et guerres futures : les armées de terre face aux évolutions technologiques », *Cahiers de l'IRSEM* n°12, 2012.

Waël Salem-Jarno, « Les armées face aux limites du "technologisme" », *LePoint.fr*, 18 avril 2017.

Peter W. Singer, *Wired for War*, New York, 2009.

Paul J. Springer, *Outsourcing War to Machines: The Military Robotics Revolution*, Santa Barbara, Praeger Security International, 2018.

Jack Watling, « Automation Does Not Lead to Leaner Land Forces », *War On The Rocks* du 7 février 2024.

Id., « The Mirage of Interconnected Battlefield », *RUSI*, 21 janvier 2022.

Fabrice Wolf, « Le technologisme est-il le pire ennemi de l'efficacité militaire ? », *Metadefense.fr*, 7 février 2019.

Mykhaylo Zabrodskyi, Jack Watling, Oleksandr V. Danylyuk et Nick Reynolds, « Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine : February-July 2022 », *RUSI*, 30 novembre 2022.

Internet

- ✕ @CDECAdT
- ▶ @cdecthink-tankdelarmedeterre
- in @CDEC – Think Tank de l'armée de Terre
- 🌐 www.terre.defense.gouv.fr/cdec

Intranet

- ▶ <https://deftube.intradef.gouv.fr/channels/#cdec>
- 🌐 <https://portail-cdec.terre.defense.gouv.fr>
- 🌐 Télécharger le document.

Comité de rédaction

Rédacteur : lieutenant (R) Calixte Wagner / Pôle études et prospective / Bureau anticipation et innovation.

Relecture : chef d'escadrons Henry Bataille et madame Gabrielle Bredon / Pôle études et prospective / Bureau anticipation et innovation.



Commandement du combat futur
1, place Joffre – Case 53
75007 Paris SP 07