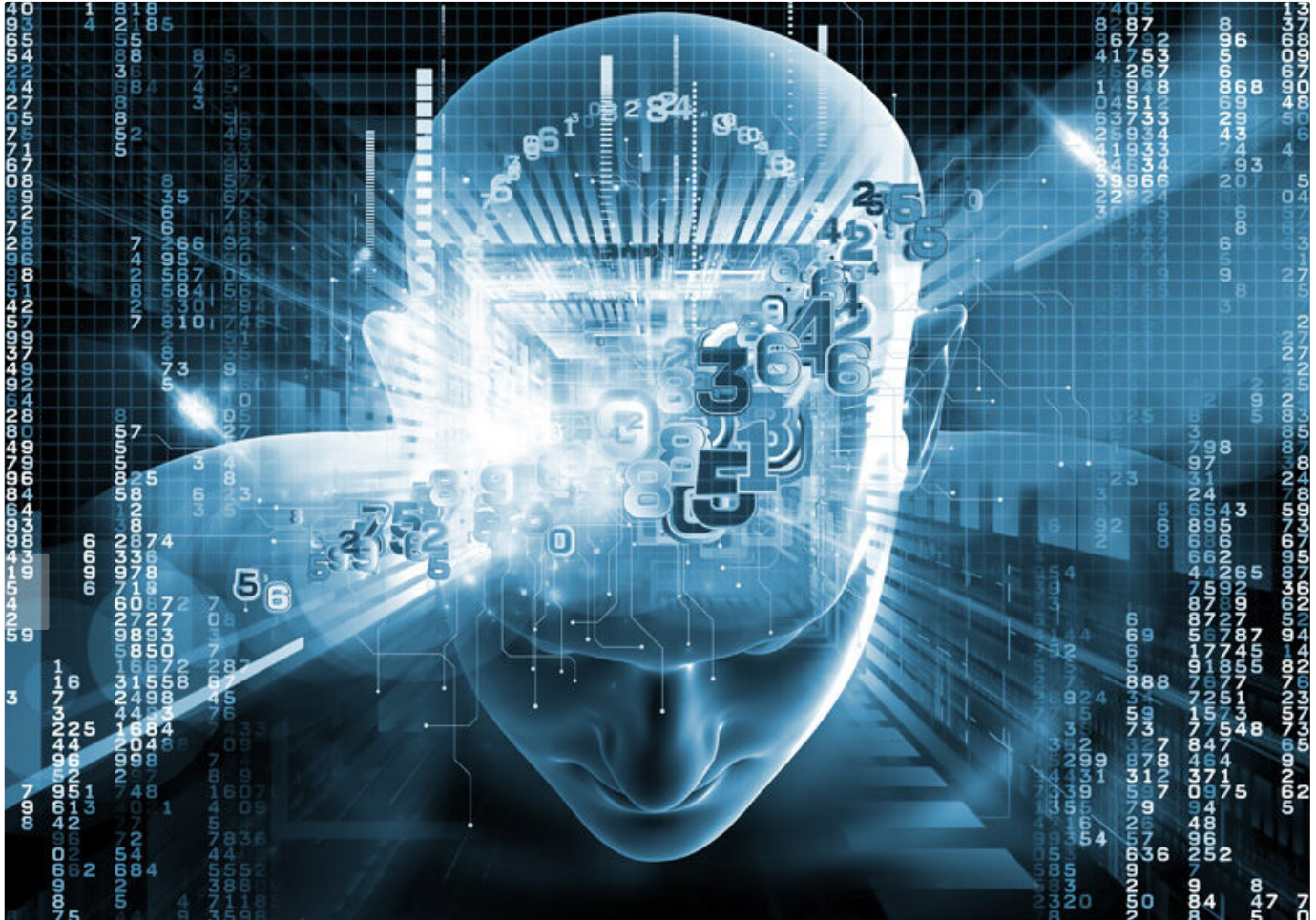


La guerre cognitive : agir sur le cerveau de l'adversaire

David Pappalardo | 9 décembre 2021 | ARTICLES | 



Début 2020, les auteurs Hervé Le Guyader et August Cole publiaient pour le NATO Innovation Hub [un essai-fiction](#) dans le but de promouvoir le « champ cognitif » comme potentiel 6^e domaine d'opération de l'OTAN au côté des milieux terrestre, aérien, naval, extra-atmosphérique et cyber. Dans la foulée, le Commandant stratégique pour la transformation lançait des travaux en vue d'établir la supériorité cognitive sur l'adversaire. Parallèlement, en juillet 2021, la *Red Team défense* – un programme mettant en relation des auteurs de science-fiction avec des militaires pour imaginer les menaces futures – proposait au ministère des Armées un scénario intitulé « [Chronique d'une mort culturelle annoncée](#) ». Ce dernier met en scène une opération militaire en 2050, où la notion de guerre cognitive est poussée à l'extrême : alors que la société est divisée en zones de réalité alternative communautaires (« [safes sphere](#) »), les armées françaises doivent « sécuriser le réel » face à un adversaire capable de modifier les comportements collectifs à grande échelle par des actions de déception, de subversion ou de manipulation de l'information.

Comme l'illustrent ces exemples, la notion de guerre cognitive a le vent en poupe dans la réflexion stratégique, bien que sa définition ne fasse pas encore l'objet d'un consensus. Face à cet engouement, il est légitime de se demander si elle n'est pas le ressac stratégique d'une grammaire ancienne et si elle se distingue des [opérations d'influence psychologiques](#), ou des « guerres de l'information » (notions elles-mêmes discutées).

Relevant d'une approche pluridisciplinaire combinant sciences sociales et nouvelles technologies, la guerre cognitive vise à altérer directement les mécanismes de compréhension du monde réel et de prise de décision pour déstabiliser ou paralyser un adversaire : en d'autres termes, elle vise à agir sur le cerveau de l'adversaire puisque c'est là que s'y gagnent les guerres, y

compris « avant la guerre », en écho à [la vision stratégique](#) du chef d'état-major des armées françaises.

Agir sur le cerveau de l'adversaire pour vaincre : un problème ancien

À première vue la guerre a toujours engagé le cœur et l'esprit. Selon [Clausewitz](#), d'un « acte de violence destiné à contraindre l'adversaire à notre volonté ». De même, [Hervé Coutau-Bégarie](#) rappelle que la stratégie est « une dialectique des intelligences dans un milieu conflictuel » où chaque camp essaie d'anticiper les réactions de l'autre pour prendre l'avantage. Au regard de l'histoire militaire et de la pensée stratégique, l'affirmation du docteur [James Giordano](#) selon laquelle « le cerveau humain est devenu le champ de bataille du XXI^e siècle » est en ce sens discutable puisque l'action sur le cerveau, dans la dialectique stratégique, a toujours constitué un élément structurant.

En outre, les opérations de simulation, de dissimulation, ou d'intoxication sont aussi vieilles que la guerre et consistent à jouer sur les perceptions de l'adversaire afin de le tromper sur nos intentions, nos capacités réelles et sur notre stratégie. Dans son ouvrage [La Ruse et la Force](#), Jean-Vincent Holeindre explique par exemple que « la ruse s'est imposée dans l'histoire de la stratégie, non seulement comme procédé tactique fondé sur la dissimulation et la tromperie, mais aussi comme une qualité intellectuelle inspirant la planification stratégique et l'adaptation à des situations d'incertitudes ». En ce sens, la stratégie est avant tout « une science de l'autre » par laquelle il s'agit de pénétrer dans le cerveau de son adversaire.

Enfin, utiliser des informations fausses pour obtenir un avantage sur son adversaire n'a rien de nouveau dans l'histoire de la stratégie. Churchill aurait par exemple dit à Staline qu'« [en temps de guerre, la vérité \[était\] si précieuse qu'elle \[devait\] être protégée par un rempart de mensonges](#) ». La subversion était également au cœur de la dialectique Est-Ouest pendant la Guerre froide.

Toutefois, révolution numérique a exacerbé la compétition dans le champ informationnel, donnant une prime de viralité au spectaculaire au détriment de l'empirique : « [la vérité cède \[ainsi\] le pas à la vraisemblance, le réflexe à la réflexion](#) ». Ce constat est partagé dans [l'Actualisation Stratégique](#) du Ministère des Armées publiée en janvier 2021 : la manipulation de l'information y est présentée comme un élément clé des stratégies hybrides mises en œuvre par nos adversaires, pouvant déboucher sur une forme de « subversion sourde » à des fins d'influence, de paralysie ou de confusion. En écho, à l'occasion de la présentation de la [doctrine militaire de lutte informatique d'influence](#) à Paris le 20 octobre 2021, la ministre des Armées Florence Parly affirme ainsi que l'information fausse, manipulée ou subvertie est une arme qui utilisée à bon escient, permet de gagner sans combattre. En conséquence, la lutte contre les agressions informationnelles est désormais une priorité pour les Armées, cette aptitude devant être développée pour ne pas subir les manœuvres de l'adversaire.

En partant de ce triple constat (1- la guerre est une dialectique des volontés et des intelligences ; 2- La stratégie est « une science de l'autre » où l'on doit rentrer dans le cerveau de l'adversaire, 3- l'information est une arme pouvant offrir un avantage stratégique sur l'adversaire), qu'apporterait de neuf cette notion de guerre de la cognition à la pensée stratégique ?

La guerre cognitive par l'exploitation des fonctions concurrentes du cerveau

La cognition recouvre l'ensemble des mécanismes combinant raisonnement, émotions et expériences sensorielles qui permettent de comprendre le monde réel pour y agir. Elle est à la base de sa représentation et de la conduite de l'action dans ce monde, en fonction de son anticipation. Elle est donc un élément majeur du processus de « prise de décision », au cours duquel notre cerveau met en concurrence des fonctions différentes : nos heuristiques intuitives (mobilisables rapidement, mais où se logent nos biais) et nos stratégies logiques (plus lentes et coûteuses en énergie), sans qu'il y ait une hiérarchie entre les deux (chacune s'appliquant à des situations différentes). Il s'agit là de ce que le psychologue Daniel Kahneman appelle respectivement le système 1 (heuristique) et le système 2 (raisonnement) dans son livre [Thinking, Fast and slow](#). Toute prise de décision nécessite un arbitrage entre ces fonctions concurrentes, pouvant nécessiter l'inhibition de nos intuitions pour ne pas devenir la proie de nos biais. [Olivier Houdé](#) qualifie ce mécanisme d'inhibition et de contrôle exécutif de notre cerveau de système 3 : c'est lui qui permet la vicariance dans les circuits de l'intelligence, conçue alors comme « une capacité d'adaptation entre l'attention et l'inhibition ».

La conflictualité dans le champ cognitif vise ainsi à exploiter ces fonctions concurrentes et la rationalité limitée des différents acteurs (biais cognitifs) à des fins stratégiques afin de provoquer des distorsions des représentations, altérer la décision et ainsi faire dévier la manœuvre stratégique la mieux planifiée. Les effets recherchés ne se limitent ainsi pas au contrôle de l'information, mais bien au contrôle de la fonction exécutive et d'arbitrage de notre cerveau lui-même. En ce sens, le cadre dépasse le seul champ de la lutte informationnelle : agir sur l'information, c'est uniquement agir sur la donnée qui nourrit la cognition. Or, l'objectif est ici d'agir non seulement sur ce que pensent les individus, mais aussi sur la façon dont ils pensent, conditionnant par là même la manière dont ils agissent.

Dans une récente étude réalisée avec le soutien de l'état-major des armées et de l'OTAN, [l'École Nationale Supérieure de Cognitique](#) offre un éclairage sur les déterminants du *cognitive warfare*. Alliant sciences dures et sciences humaines et sociales, l'ENSC défend l'idée que les progrès dans ce domaine doivent passer par la convergence entre les travaux sur le cerveau (neurosciences) et les travaux sur les technologies. Selon le professeur Bernard Claverie et le lieutenant-colonel François du Cluzel, la guerre cognitive est ainsi nécessairement associée à d'autres formes et domaines d'action pour atteindre le ou les cerveaux-cibles, tels le *cyber warfare* et l'*information warfare* ; elle correspond ainsi à

« l'art d'utiliser les technologies pour altérer la cognition de cibles humaines, le plus souvent à leur insu et à l'insu de ceux qui seraient en charge d'éviter, minimiser, contrôler les effets recherchés, ou dont un contrôle possible serait dépassé ou trop tardif »

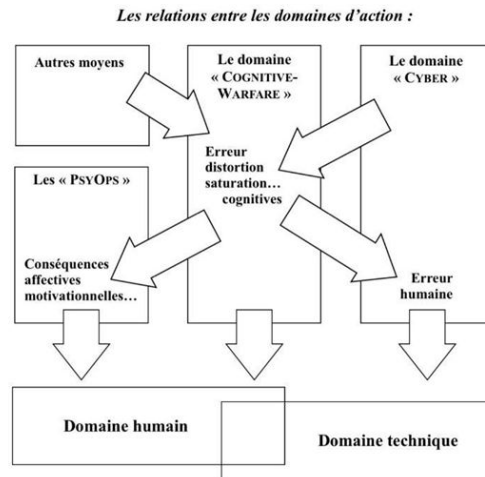


Schéma : Guerre cognitive, les relations entre les domaines d'action

La cognitique s'apparenterait ainsi au traitement automatique de la cognition (de même que l'informatique est « *le traitement automatique de l'information* »). Pour autant, l'approche n'est pas uniquement technologique : elle répond aux nouvelles exigences du [Human Autonomy Teaming](#) (HAT) devant permettre de tirer parti de la précision et de la vitesse des technologies numériques (IA, Big Data analytics etc.) tout en décuplant l'agilité et la créativité de l'intelligence humaine.

Vers des structures de commandement adaptées à la dimension cognitive de la conflictualité

On comprend dès lors aisément que la guerre cognitive concerne essentiellement (mais pas uniquement) les travaux sur le commandement et le contrôle des opérations (C2) : la maîtrise de l'information (*information dominance*) dans un environnement cyber sécurisé (*cyber confidence*) doit permettre d'obtenir la supériorité décisionnelle (*decision superiority*). Pour ce faire, il est possible d'identifier trois lignes d'effort.

La première concerne la nécessité de se prémunir de ses propres certitudes, individuelles et collectives. Cela passe tout d'abord par la connaissance et l'identification – autant qu'il en soit possible – de nos biais cognitifs qui préconditionnent nos schémas mentaux. Selon la belle formule de Jean d'Ormesson, « [penser, c'est d'abord penser contre soi-même](#) ». La question de l'éducation et de la formation des militaires est ainsi cruciale afin de mieux les préparer à ces enjeux. Cela nécessite une remise en question permanente favorisée par une approche sociale et psychologique de la conflictualité. Comme l'explique également [Robert Jervis](#), la mauvaise compréhension des idées ou des valeurs de l'adversaire, la présomption qu'il nous verra comme nous nous voyons et plus généralement le mépris de l'altérité, sont autant de puissants facteurs d'instabilité dans les relations conflictuelles.

En outre, il est nécessaire de s'émanciper de l'utopie d'une vision parfaite du champ de bataille qui serait rendue possible par la seule technologie. En effet, les moyens technologiques ne dissipent pas toujours le brouillard de la guerre (*Fog of War*). Ils peuvent au contraire ajouter de la complexité au détriment de l'efficacité militaire si l'on ne parvient pas à maîtriser le déluge informationnel (*Fog of More*). Par ailleurs, les biais se logent également dans les algorithmes ou les bases de données utilisées « pour rendre le futur prévisible ». C'est ainsi la [qualité de l'organisation qui doit prévaloir sur les solutions technologiques dans la pratique de l'information](#). Pour les armées, une qualité essentielle du C2 réside précisément dans l'intégration équilibrée entre l'homme et le système en vue de distiller la clarté de la complexité dans cette guerre de la cognition. Pour paraphraser [Bruno Patino](#), les lumières philosophiques ne doivent pas s'éteindre au profit des signaux numériques.

La seconde ligne d'effort concerne la défense contre les agressions informationnelles permanentes et l'exploitation opportuniste par un adversaire de nos biais cognitifs, susceptibles de contraindre notre processus décisionnel et de nous

paralyser. Nos grands compétiteurs ont compris les vulnérabilités de nos sociétés, auxquelles nos armées appartiennent. Au moins trois défis peuvent être ainsi relevés. Le premier concerne la rationalité limitée des acteurs : goût pour les récits contradictoires et les « [friandises cognitives](#) » qui détournent notre attention et entravent notre jugement ; [propension au doute systématique](#), etc. Le second est lié à notre système de valeurs, qui promeut la libre circulation des idées ; le troisième rend plus problématique encore le second puisqu'il est lié à la grande porosité des frontières informationnelles (institutionnelles et étrangères).

On comprend ainsi que la guerre de la cognition passe par une approche globale, multimilieux, multichamps et interministérielle, faisant la promotion d'une meilleure intégration entre les domaines cyber et les champs informationnels (l'information est un actif, et en cette qualité elle doit être défendue). Au niveau strictement militaire, nos architectures C2 doivent demeurer résilientes, c'est-à-dire pouvoir tirer parti des nouvelles technologies tout en limitant au maximum les dépendances et la dégradation des expertises humaines. La cyber sécurisation des réseaux et des contenus est à cette aune essentielle.

La guerre offensive dans le champ cognitif constitue le troisième axe d'effort, même s'il soulève des questions éthiques qui ne doivent ni être éludées ni paralyser l'action dans ce champ. Ainsi, [lors de son audition devant le Congrès le 30 avril 2021](#), le chercheur américain Herbert Lin (*Hoover Institute*) faisait remarquer avec amusement que les contraintes éthiques que s'imposait le département de la Défense avaient abouti au paradoxe suivant : *"it is easier to get permission to kill terrorists than it is to lie to them."* La conduite d'une véritable guerre cognitive offensive ne s'affranchira pas d'une réflexion poussée sur l'encadrement éthique nécessaire, tout en restant cohérente d'un point de vue stratégique.

L'un des enjeux de la guerre cognitive consiste par conséquent à réhabiliter la ruse et la surprise dans la stratégie par une opacification préalable de la cognition de l'adversaire (simulation, dissimulation, intoxication). Par conséquent, l'organisation du C2 devra évoluer pour favoriser une meilleure intégration des effets dans tous les milieux (terre, air, mer, extra-atmosphérique) et tous les champs (cyber et informationnel). À titre d'exemple, la création des task-force multidomaines par l'US Army est intéressante puisqu'on trouve en leur sein un bataillon I2CEWS (*Intelligence, Information, Cyber, Electronic Warfare and Space*) au côté des bataillons de feux dans la profondeur et de défense surface-air.



La guerre cognitive consiste à pénétrer le cerveau de l'adversaire pour influencer sa prise de décision, créer de la confusion et *in fine* paralyser son action afin d'emporter la victoire. La révolution numérique exige d'y prêter une attention nouvelle au travers de la militarisation de neurosciences et de l'intégration croissante des effets dans tous les milieux et tous les champs. L'un des objectifs est dès lors de faire émerger un C2 adapté à la dimension cognitive de la conflictualité multimilieux et multichamps, associant harmonieusement le jugement humain et les technologies numériques pour être en mesure de surprendre sans être surpris. La France doit ainsi continuer à approfondir la question avec les Alliés, notamment en participant activement aux travaux de l'OTAN.

Est-ce à dire qu'il est nécessaire de créer un nouveau domaine ou un nouveau champ de conflictualité ? Rien n'est moins sûr et le sujet doit être exploré plus avant : un découpage toujours plus fin n'est pas nécessairement synonyme d'une meilleure prise en compte de la problématique, ce d'autant plus lorsque l'ambition est au contraire de mieux intégrer les effets produits à des fins d'efficacité militaire.

Quoi qu'il en soit, l'intensification de la guerre cognitive par les nouvelles technologies est aujourd'hui manifeste tout au long du continuum compétition – contestation – affrontement, où l'adversaire cherche à nous intimider sans cesse. Pour « [gagner la guerre avant la guerre](#) », il est nécessaire de se préparer à remporter la bataille de la cognition en se prémunissant de ses propres certitudes, en se protégeant contre les agressions qui visent nos perceptions, mais aussi en s'autorisant à agir sur le cerveau de l'adversaire grâce à la simulation, l'intoxication ou la dissimulation.

Les propos tenus dans cet article n'engagent pas la DGRIS ni le ministère des Armées.

— . — — . — . — . .

David Pappalardo

David Pappalardo ([@DavPappa](#)) est un officier de l'armée de l'air et de l'espace servant actuellement à la Direction Générale des Relations Internationales et de la Stratégie du ministère des Armées. Ancien pilote de Mirage F1 et de Rafale, il est crédité de 2 200 heures de vol et 134 missions de guerre au Sahel, en Afghanistan, en Libye et au Levant. Chef de patrouille et de mission, il a notamment commandé le Régiment de chasse 2/30 « Normandie-Niémen » sur la base aérienne de Mont-de-Marsan entre 2016 et 2017.

Comment citer cette publication

David Pappalardo, « La guerre cognitive : agir sur le cerveau de l'adversaire », *Le Rubicon*, vol. 1, 9 décembre 2021 [<https://lerubicon.org/la-guerre-cognitive/>].