NOTE DE RECHERCHE PROSPECTIVE

FORUM de la pensée mili-terre

Armée de terre
Centre de doctrine et d'enseignement du commandement

Champs immatériels, un combat de l'information

Céline Gojon
rédactrice au pôle études et prospective

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

RÉSUMÉ.

Dans un contexte de retour de la haute intensité, les différents champs de conflictualité que sont le cyberespace, l'environnement électromagnétique et les perceptions ont un rôle grandissant. Nos compétiteurs actuels et à venir seront de plus en plus en mesure de nous défier dans ces espaces, qui incluent des champs de bataille variés et aussi nouveaux que les réseaux sociaux par exemple.

L'adaptation de la capacité de la France à combattre dans les différents champs de la conflictualité est une préoccupation permanente, nos modes d'action peuvent se perfectionner pour intégrer cette évolution de la conflictualité. S'ils sont actuellement réunis sous la bannière des « champs immatériels », ce terme ne permet ni de refléter la réalité du terrain, ni même d'offrir une cohérence dans leurs relations réciproques. L'approche américaine, basée sur le nouveau concept de *Multi-Domain Operations* (MDO), permet d'entrevoir une nouvelle façon d'aborder ces trois champs dits « immatériels », et de comprendre les évolutions en cours dans la réflexion doctrinale aux États-Unis.

1. Un changement de paradigme nécessaire : champs immatériels ou environnement informationnel ?

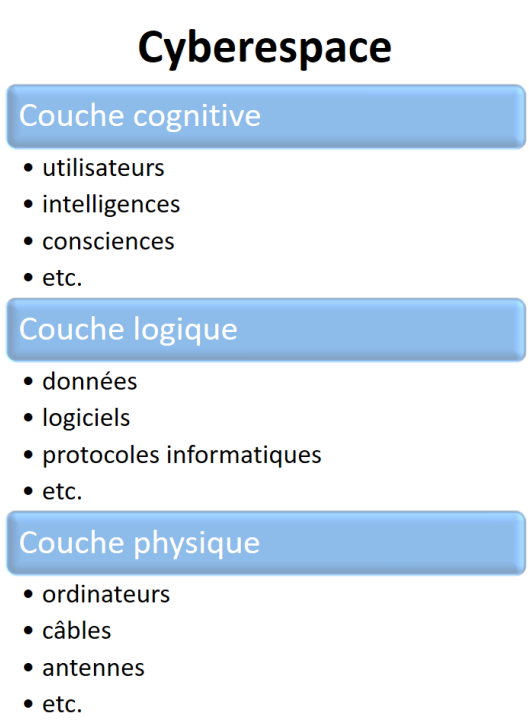
S'il n'existe pas, à l'heure actuelle et au niveau mondial, de définition consensuelle des champs immatériels dans le domaine de la recherche et dans les doctrines militaires[1], il est de plus en plus souvent lu qu'ils regroupent le cyberespace, l'environnement électromagnétique et l'ensemble du champ des perceptions[2]. En France, le champ des perceptions est parfois remplacé par l'information, ce qui pose des problèmes de chevauchement entre ces trois périmètres (le cyberespace et l'environnement électromagnétique sont aussi des champs informationnels). À l'étranger, certains pays amalgament tout cela avec des opérations dans l'espace, le renseignement, voire les opérations de contre-insurrection ou de diversion, sans que la logique soit évidente.

[1] Action terrestre future définit les champs immatériels comme la convergence de l'environnement informationnel, du cyberespace, de l'environnement électromagnétique sans lui donner plus d'essence.
[2] Michel Goya, Isabelle Dufour, « Dans la perspective d'affrontement de haute intensité, comment intégrer dans le combat aéroterrestre des actions sur les champs immatériels ? », *Observatoire de l'armée de Terre 2035*, Fondation pour la recherche stratégique, 21 avril 2020.

1.1. La remise en question de la notion et de l'organisation des champs immatériels.

a. Une séparation entre immatériel et matériel peu pertinente ?

Le cyberespace, à la fois espace et milieu à part entière, est défini dans la doctrine française comme « l'espace de communication constitué par l'interconnexion mondiale d'équipement de traitement automatisé des données numériques […] Le cyberespace est aussi un milieu immatériel qui n'existe et n'a de sens que par l'information (au sens générique du terme)[3] ». L'environnement électromagnétique quant à lui se répartit entre le domaine des SIC (systèmes d'information et de communication) avec les liaisons hertziennes de données (Wifi, radio, FH, *etc.*) et de la guerre électronique, cette dernière étant définie comme « tout ce qui a trait aux opérations de combat effectuées dans l'environnement électromagnétique[4] ». Enfin, la revue stratégique définit la conduite des opérations d'influence comme : « les aptitudes qui désignent un ensemble de procédés qui visent à susciter l'adhésion, légitimer ou favoriser l'action de notre force avant, pendant et après les opérations ; elles s'insèrent dans une approche globale des opérations et se conduisent dans les champs matériels et immatériels[5] ».



Si ces trois champs sont tous étiquetés, en première approche, comme « champs immatériels » (remplaçant parfois le terme « virtuels », souvent utilisé, non sans problèmes), en revanche leur définition indique déjà les limites d'une telle appellation. Le cyberespace, tout comme l'environnement électromagnétique et le champ des perceptions peuvent être le support d'opérations ayant un impact physique, donc matériel : ainsi, le virus informatique Stuxnet a entraîné la mise hors service des centrifugeuses bien réelles et matérielles du programme nucléaire iranien. Mais encore, tuer un ennemi, détruire ses moyens de production et de transmission de l'information constitue une opération dans les champs matériels ciblant toute une capacité d'influence. Détruire une antenne est très « physique » et constitue une opération de cyberdéfense concourant au combat de la guerre électronique. Tout comme le champ des perceptions se définit à la fois par des éléments physiques et immatériels[6], le cyberespace est défini comme regroupant trois couches, dont une couche physique qui s'ajoute à la couche logique et cognitive. Celle-ci se définit comme les « équipements des systèmes informatiques et de leurs réseaux ayant une existence matérielle et, pour certains d'entre eux, une existence électromagnétique[7] ». Ces couches sont intrinsèquement liées : des effets sur la couche « matérielle » du cyberespace peuvent donc se répercuter sur les couches « immatérielles », et réciproquement.

[3] Définition de l'ANSSI.
[4] Michel Goya, Isabelle Dufour, *Op. Cit.*
[5] *Revue stratégique de Défense et de sécurité Nationale*, 2017.
[6] RAND Corporation, « Requirement for Better C2 and Situational Awareness of the Information Environment », *Research Brief*, 2018.
[7] Ministère des Armées / COMCYBER. *Éléments publics de doctrine militaire de lutte informatique offensive*, 2019.

b. *Une séparation artificielle des différents champs.*

Au sein des champs immatériels, le cyberespace a longtemps été considéré comme prépondérant, car transverse. Toutefois, la doctrine française a commencé à constater que la séparation et la hiérarchisation entre ces trois champs correspondait difficilement à la réalité. La DIA-3.20(A) énonce ainsi que « les opérations dans le cyberespace se coordonnent, se complètent et se combinent avec les EMO (opérations électromagnétiques) ». Des liens existent donc.

La doctrine américaine a elle aussi mis en exergue ce constat. Le *Field Manual 3-12*, *Cyberspace and Electronic Warfare Operations* (CEWO) de 2017, précise que le spectre électromagnétique constitue un « dénominateur commun » de la guerre électronique et de la guerre cyber[8]. Une caractéristique importante du cyberespace est que les systèmes d'info-communication en réseau y fonctionnent en utilisant le spectre électromagnétique : le but est de combiner et « synchroniser les fonctions et les capacités des opérations dans le cyberespace, de la guerre électronique et des opérations de gestion du spectre pour produire des effets complémentaires[9] ». La synergie des activités cyber-electromagnétiques *(Cyber-Electromagnetic Activities, CEMA)* a par ailleurs déjà été utilisée de façon efficiente par des pays membres de l'OTAN lors de l'opération *Atlantic Resolve*[10]. En 2018, le *Ministry of Defence* du Royaume-Uni publiait aussi une *Joint Doctrine Note 1/18* relative aux *Cyber and Electromagnetic Activities*[11] donnant ainsi davantage de crédit à un rapprochement entre cyber et guerre électronique.

L'avènement des nouvelles technologies de l'information et de la communication (NTIC) a donc permis ce rapprochement entre les télécommunications et l'informatique, reliant guerre électronique et opérations cyber[12]. Les opérations d'influence dans le champ des perceptions, permises notamment par l'utilisation de ces NTIC, reposent donc en partie sur la guerre électronique et les actions dans le cyberespace.

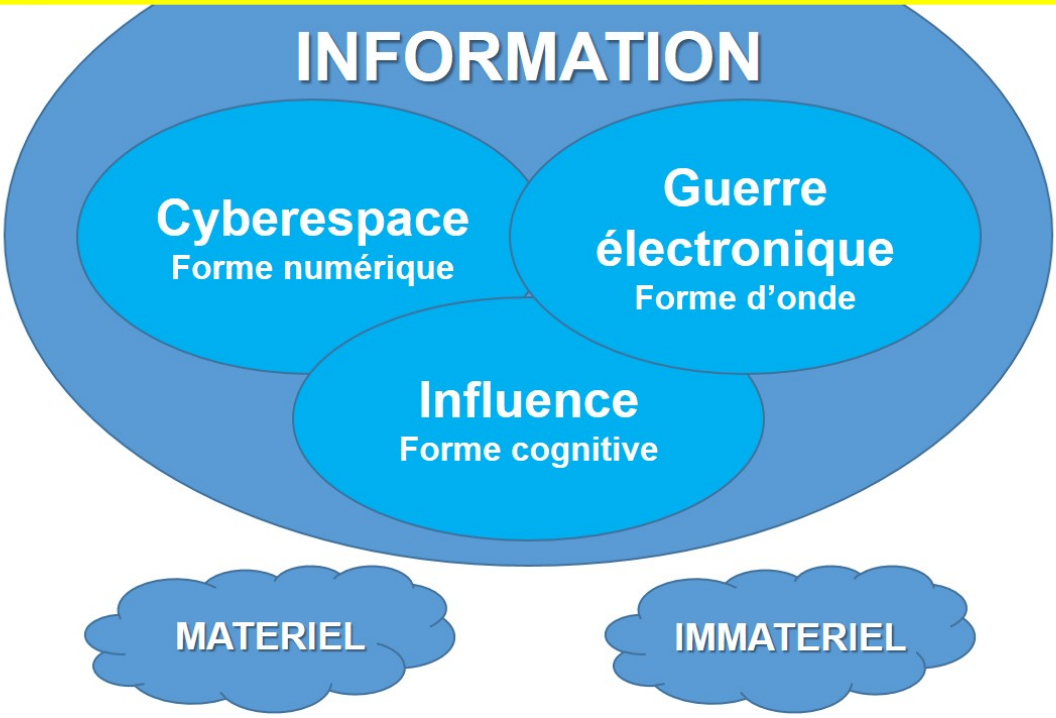
1.2. L'avènement d'un nouveau domaine dans lequel s'organisent ces champs : environnement informationnel et *information warfare*.

Dans ce contexte, il peut paraître opportun de trouver un dénominateur commun à ces trois champs, afin de mieux penser leurs relations et les effets combinés que l'on peut en tirer. Si l'on considère une approche par les effets, on se rend compte qu'ils sont en réalité liés par leur « *information-related capability* ». En particulier avec l'emploi de plus en plus massif des réseaux sociaux depuis plus de dix années, l'information redevient un domaine d'opérations majeur[13]. L'environnement informationnel est défini comme un « *aggregate of individuals, organizations and systems that collect, process, dissiminate or act on information*[14] *»*. Dans ce cadre, la guerre de l'information représenterait « toute activité destinée à acquérir données et connaissances (et à en priver l'adversaire) dans une finalité stratégique, soit par

[8] Philippe Gros, « Les opérations en environnement électromagnétique dégradé », *Fondation pour la recherche stratégique,* note n° 357/Consortium CONFLITS-2035, 18 mai 2018.
[9] Col. Prof. Zsolt Haig, PhD, Ing, « Electronic Warfare in Cyberspace », *Security and Defense Quarterly*, June 2015.
[10] Colonel Matthew Willis, lieutenant-colonel Panagiotis Stathopoulos, « Cyber-Electromagnetic Domain, The Necessity of Integrating the Electromagnetic Spectrum's Disciplines Under a Single Domain of Operations », *Joint Air Power Competence Center,* https://www.japcc.org/cyber-electromagnetic-domain/
[11] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/682859/doctrine_uk_cyber_and_electromagnetic_activities_jdn_1_18.pdf
[12] Olivier Letertre, Patrick Justel, Romain Lechâble et Stéphane Dossé, « Regards croisés sur la guerre électronique », *Focus Stratégique*, n°90, IFRI, juillet 2019.
[13] Daniel T. Kuehl, « Information Operations, Information Warfare, and Computer Network Attack. Their Relationship to National Security in the Information Age », I*nternational Law Studies*, Vol. 76.
[14] Isaac R. Porche III, Christopher Paul, Michael York, Chad C. Serena, Jerry M. Sollinger, Elliot Axelband, Endy Y. Min, Bruce J. Held « Redefining information warfare boundaries for an army in a wireless world », RAND, 2013.

des systèmes (vecteurs et moyens de traitement de l'information), soit par le contenu, en assurant une domination informationnelle[15] ».

L'information se présente souvent simultanément sous une forme numérique, sous la forme d'ondes et dans les esprits. L'information s'attaque et se défend alors par la cyberdéfense, par la guerre électronique et par les opérations d'influence dans une manœuvre unique.
La planification, l'intégration, la conduite et la coordination des opérations de guerre de l'information s'effectue dans sa dimension matérielle et immatérielle pour agir sur toutes les formes et tous les supports de l'information



L'U.S. *Army* considère comme « *information-related* » toute capacité utilisée pour créer des effets et des conditions opérationnelles souhaitables au niveau de l'environnement informationnel[16].

Or, la guerre électronique, tout comme les opérations dans le cyberespace et les opérations d'influence, contribuent à l'obtention de la supériorité informationnelle[17]. Ainsi les « opérations d'information cybernétique[18,19] » constituent une nouvelle catégorie d'opérations dans l'environnement informationnel. Déjà, l'AJP-3.10 de l'OTAN affirmait que le « *cyberspace and the electromagnetic spectrum are part of the information environment*[20] ». Ces trois champs contribuent donc activement aux actions menées dans le cadre de l'*information warfare*, concept défini comme « *conflict or struggle between two or more groups of the information environment*[21] ».

[15] Daniel Ventre (dir.), *Cyberguerre et guerre de l'information*, Lavoisier, Paris, 2010, 319 p.
[16] FM 3-13, *Information Operations*, Department of the Army, December 2016.
[17] Col. Prof. Zsolt Haig, PhD, Ing, *Op. Cit.*
[18] Dr. Glenn Alexander Crowther, « The Cyber Domain », *The Cyber Defense Review*, Fall 2017.
[19] Lieutenant General Paul M. Nakasone, Major Charlie Lewis, « Cyberspace in Multi-Domain Battle », *Cyber Defense Review*, 2017.
[20] AJP-3.10 Allied Joint Doctrine for Information Operations. November 2009. NATO Standardization Agency.
[21] « Conflit ou lute entre deux ou plusieurs groupes de l'environnement informationnel », dans TRADOC Pamphlet 525-3-1, *Op. Cit.*

2. État des lieux de la réflexion sur l'*information warfare* aux États-Unis.

L'approche américaine s'est construite face à des adversaires historiques et majeurs ayant aussi réfléchi à ces évolutions. Citons notamment le concept chinois de « guerre hors limite », et le concept russe de « guerre non linéaire », avec son corollaire doctrinal « *new generation warfare »*.

L'armée américaine regroupe de fait les champs des perceptions, le cyberespace et l'environnement électromagnétique dans les opérations d'information (*information operations, IO*) : « *There are many military capabilities that contribute to IO and should be taken into consideration during the planning process. These include: strategic communication, joint interagency coordination group, public affairs, civil-military operations, cyberspace operations (CO), information assurance, space operations, military information support operations (MISO), intelligence, military deception, operations security, special technical operations, joint electromagnetic spectrum operations, and key leader engagement*[22] ».

L'*Army* considère donc le mot information au sens large : que ce soit le volet numérique (le cyberespace), le volet cognitif (opérations d'influence ou PSYOPS) ou encore au niveau des ondes (environnement électromagnétique). Dans le contexte d'avènement du nouveau concept *Multi-Domain Operations* (MDO), ces trois champs de la conflictualité sont corrélés en vue d'effets conjoints dans le cadre de l'*Information Warfare.* Cela entraîne des changements organisationnels.

2.1. Le *Multi-Domain Operations* et l'évolution de l'imbrication des différents champs.

L'U.S. *Army Training and Doctrine Command* (par le TRADOC) paru en 2018, The U.S. *Army in Multi-Domain Operations* 2028[23], mentionne plus de 40 fois l'*information warfare*[24].

Le MDO peut être vu comme les « opérations menées dans de multiples domaines et espaces contestés pour surmonter les forces d'un adversaire (ou d'un ennemi) en lui présentant plusieurs dilemmes opérationnels et/ou tactiques par l'application combinée d'une posture de forces calibrée, l'emploi de formations multi-domaines et la convergence des capacités entre domaines, environnements et fonctions, dans le temps et l'espace pour atteindre des objectifs opérationnels et tactiques[25] ». À ces niveaux tactique et opérationnel, il est donc nécessaire de combiner les capacités et les effets dans les différents domaines (ce terme étant défini comme « tout espace » opérationnel potentiel par lequel le système cible peut être influencé - non seulement les domaines terrestre, maritime, aérien et spatial, mais aussi les domaines virtuel (information et cybernétique) et humain (cognitif, moral et social)[26] »). En ce sens, le MDO n'est pas une modernisation de l'interarmées, mais bien une tentative de descendre au plus bas niveau une combinaison d'opérations offensives et

[22] « De nombreuses capacités militaires contribuent aux OI et doivent être prises en considération lors du processus de planification. Il s'agit notamment de la communication stratégique, du groupe de coordination inter agences, des affaires publiques, des opérations civilo-militaires, des opérations dans le cyberespace, de l'assurance de l'information, des opérations spatiales, des opérations de soutien de l'information militaire, du renseignement, de la diversion militaire, de la sécurité des opérations techniques spéciales, des opérations conjointes sur le spectre électromagnétique et de l'engagement des principaux dirigeants » dans JP 3-13, *Information Operations*, novembre 2014.

[23] TRADOC Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations* 2028, 2018, p.GL-7, https://www.tradoc.army.mil/Portals/14/Documents/MDO/TP525-3-1_30Nov2018.pdf

[24] Kyle Rempfer, « Army Cyber lobbies for name change this year, as information warfare grows in importance », *ArmyTimes,* 16 octobre, https://www.armytimes.com/news/your-army/2019/10/16/ausa-army-cyber-lobbies-for-name-change-this-year-as-information-warfare-grows-in-importance/

[25] TRADOC Pamphlet 525-3-1, *Op. Cit.*

[26] Joint Chiefs of Staff, *Capstone Concept for Joint Operations, Version 2.0* Washington, DC: US Government Printing Office, 2005.

défensives dans tous les champs à la disposition du chef tactique, pour compléter ses missions « cœur de métier » terrestre (ceci est également valable pour la Marine et l'armée de l'Air et de l'Espace).

Cette nouvelle doctrine a pour but d'exploiter les « fenêtres de supériorité », en combinant dans une approche par les effets, les capacités de différents domaines, notamment dans l'environnement informationnel[27]. Ce dernier constitue donc bien en quelque sorte le dénominateur commun pour les trois champs considérés.

Un exemple de cette complémentarité est le fonctionnement du 915th *Cyber Warfare Battalion*, destiné à fournir au niveau tactique à la fois des capacités de cyber-opérations mais aussi de guerre électronique, pour mettre en œuvre des opérations d'information. Il existe donc des évolutions organisationnelles liées cette nouvelle compréhension de l'*Information Warfare*.

2.2. Des transitions institutionnelles comme reflet de ces changements : le cas de l'ARCYBER.

Les réflexions actuelles au sein de l'ARCYBER (*U.S. Army Cyber Command*) illustrent cette nouvelle compréhension de l'environnement informationnel. « L'*Information advantage* » et la « *decision dominance »* sont deux nouveaux volets en développement[28]. Le général Stephen Fogarty, commandant cette entité, a déclaré opérer et manœuvrer tous les jours au sein de l'environnement informationnel[29].

Dans ce contexte, la volonté d'un changement de nom de l'organisation en *Army Information Warfare Command* est significative. Une telle évolution entraînerait une augmentation des moyens et des capacités d'ARCYBER, incluant non seulement le commandement cyber mais aussi le commandement des autres champs de l'environnement informationnel.

De plus, les rivalités se nourrissant des possibilités « info-centrée », - comme l'illustrent l'implication russe dans l'élection présidentielle américaine en 2016, la désinformation durant la crise du *COVID-19*, ou encore le poids pris par les réseaux sociaux de Daech en 2015 - l'entité cherche à se transformer et se moderniser pour envisager des opérations aux niveaux tactique, opérationnel et stratégique[30]. Cette évolution redonne une importance considérable à l'information et à l'influence, tout en accompagnant le concept de MDO dans la recherche de convergence et de complémentarité des différents domaines.

Cette situation lève le voile sur un changement de paradigme qui a lieu au sein de l'armée américaine à propos de la guerre de l'information, qui réunit désormais les domaines d'opérations cyber, de guerre électronique, de guerre psychologique et d'opérations dans l'espace, et marque la volonté de mettre en place une véritable approche par les effets[31].

---

[27] Heftye Erik. « Multi-Domain Confusion: all Domains Are Not Created Equal ». *RealClear Defense*, 26 mai 2017.
[28] PotoMac Officers Club, « ARCYBER to move beyond tradition cyber operations », 30 septembre 2020, https://potomacofficersclub.com/arcyber-to-move-beyond-tradition-cyber-operations/
[29] Kyle Rempfer, *Op. Cit.*
[30] Lieutenant General Stephen G. Fogarty, Colonel (Ret.) Bryan N. Sparling, « Enabling the Army in an Era of Information Warfare », *The Cyber Defense Review*, summer 2020.
[31] Mark Pomerleau, « How the Defense Department is reorganizing for information warfare », *C4ISRNET*, 2§ juillet, https://www.c4isrnet.com/smr/information-warfare/2020/07/26/how-the-defense-department-is-reorganizing-for-information-warfare