ECOLE DE GUERRE

PROMOTION *VERDUN*

2015 -2016

Les cyberattaques comme pilier de la guerre hybride

Commandant Luiggi Jean Sun

Sous la direction du

Lieutenant-colonel Olivier Entraygues

Responsable de programme

à l'institut de recherche stratégique de l'école militaire

Abstract / Résumé

LES CYBERATTAQUES COMME PILIER DE LA GUERRE HYBRIDE, par le commandant Jean S. Luiggi, Armée de Terre, 18 pages (corps de texte hors annexes).

The concept of hybridity, applying to warfare or threats, is nowadays a common mantra in many strategic analyst and expert assumptions. The politically-backed acceptance of this term makes it relevant in our Western societies, when new perceptions of threats cumulate with a new informational environment. In the latter, the struggle between state and non-state actors points out the weaknesses and opportunities created by cyberspace. The information sphere of influence is of paramount importance in a connected world. Future threats will not only attempt to thwart any regional alliance and state actors, but will also take advantage of their lack of long lasting strategic goal and efficient narrative, allowing their own, even irrational, to prevail at the end. Relevant or not in the wording, hybrid warfare is worth studying as it represents the new form of conflict to come, either state-backed or not, blending classic warfare and irregular warfare, with cyberattacks as obvious force multiplier.

Le concept d'hybridité, se rapportant aux conflits ou menaces, s'avère être de nos jours un leitmotiv commun de nombreux analystes stratégiques et une source d'hypothèses d'experts. La caution politique de ces termes en fait un élément pertinent pour nos sociétés Occidentales, alors que de nouvelles perceptions de menaces s'ajoutent à un environnement informationnel nouveau. Dans ce dernier, la lutte entre acteurs étatiques et non étatiques souligne les faiblesses et opportunités créées par le cyberespace. La sphère d'influence informationnelle est d'une importance majeure dans un environnement mondialement connecté. Les menaces futures ne se contenteront pas de déjouer les plans des alliances et des acteurs étatiques mais profiteront de leur manque de communication efficace et de vision stratégique de long terme, pour offrir toute latitude à leur propre propagande, aussi irrationnelle soit-elle, à supplanter les autres. Qu'elle soit pertinente ou non dans sa sémantique, la guerre hybride mérite d'être étudiée en tant que nouvelle forme de conflictualité, soutenue par des États ou d'autres acteurs, en ce qu'elle mêle guerre classique et irrégulière, où les cyberattaques font manifestement figure de démultiplicateurs de puissance.

LES CYBERATTAQUES COMME PILIER DE LA GUERRE HYBRIDE

Introduction

« *Alors que nous essayons de disséquer cette guerre hybride ou non-conventionnelle, que nous voyons menée aujourd'hui, les choses nouvelles résident dans la façon dont ces outils que nous connaissions auparavant sont rassemblés et utilisés de façon nouvelle […]* » Les propos du SACEUR, le Général Breedlove, dans son discours du 23 mars 2015 au *Brussels Forum*, énoncent à eux seuls une des ambiguïtés de la guerre hybride. Le phénomène hybride est-il un phénomène nouveau ou ancien ? Choisir d'orienter une recherche sur la guerre et les menaces hybrides revient à comprendre ce que ces concepts impliquent. Les cyberattaques, actions hostiles et prédatrices de la sphère informationnelle, prises isolément n'ont de sens que par la projection de la volonté de puissance d'individus et petits groupes criminels isolés. En revanche, la recherche du lien qui unit les cyberattaques aux guerres et menaces hybrides, permet de percer à jour le fonctionnement particulier de cette nouvelle forme de conflit. Ce nouveau visage de la guerre agit par procuration et cherche ainsi à dissimuler son action.

La recherche des armes secrètes et des technologies innovantes a souvent été poursuivie pour gagner une guerre. Toutefois, exagérer l'importance d'une arme pour son seul aspect technique s'avère contreproductif. La simple mise en place de nouvelles méthodes de combat suffit à concrétiser certaines victoires. Dans le cas présent, le concept de guerre hybride ne fait pas consensus. Phénomène novateur[1], il s'oppose à des méthodes de conflits classiques et symétriques. Comme le souligne toutefois le Major Brian P. Fleming de l'*US Army* : *« ignorer les menaces hybride émergentes ou les traiter avec un certain mépris intellectuel revient à accepter un risque stratégique, dans la mesure où elles visent à créer une opportunité stratégique*[2]*[…]»* Les outils mis en place pour lutter contre les notions plus communément admises de guerre irrégulière et guerre asymétrique, comme l'approche globale[3], favorisant l'approche systémique[4] de ces questions peuvent manquer l'adversaire.

[1] Novateurs dans les termes mais non nouveaux : la guerre hybride est un mélange d'autres notions comme la guerre irrégulière et la guerre « *hors limites* » définie par les colonels Qiao Liang et Wang Xiangsui.. Qiao L, Wang X, *La guerre hors limites,* trad. Denès H., Paris, rivages poche, 2006, p. 95.
Quant aux cyberattaques, la première d'ampleur notable a eu lieu en 1988.

[2] Fleming, Brian P. *(Major): The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art, School of Advanced Military Studies, 2011,* p.ii.

[3] L'approche globale est mise en œuvre dans le processus de planification des opérations, notamment à l'OTAN. « *L'OTAN reconnaît que la seule voie militaire ne peut résoudre les crises et conflits».ACO COPD Interim V.2.0,* octobre 2013, p. 1-1 *[Traduction de l'auteur]*

Celui-ci, insaisissable, contournerait la puissance, pourrait user de tactiques de seuil[5], où l'intervention adverse ne serait pas déclenchée[6]. Le Centre Interarmées de Concepts de Doctrines et d'Expérimentations (CICDE) mentionne des *« champs de confrontations hybride »* et *« l'hybridité croissante des menaces[7] »* tout en fournissant une définition du concept : *« une stratégie combinant des actions conventionnelles et non conventionnelles, menées dans les champs les plus divers par des moyens militaires ou non militaires, mis en œuvre par des adversaires étatiques aussi bien que non étatiques »*. Sans les définir, le livre blanc sur la défense et la sécurité nationale 2013 évoque l'émergence de « menaces hybrides » face à nos forces[8]. La « cyberguerre », terme encore plus controversé, voit régulièrement son caractère guerrier nié, cette « arme » n'ayant pas fait couler de sang. Accepter cette sémantique présente également un danger contre lequel Erick Gartzke[9] et Eric Filiol[10] nous mettent en garde. Faut-il pour autant ignorer les effets produits sur la volonté du camp adverse ou la sidération causée aux acteurs économiques et financiers alors que certaines puissances, dont la Russie qu'étudie Yannick Harrel[11], cherchent à s'en assurer la maîtrise ? C'est également ce que Bertrand Boyer[12] s'efforce de démontrer. La guerre hybride s'épanouit sur le champ de l'information, de la subversion, et recherche les opportunités stratégiques via le cyberespace : *« les communautés virtuelles qui opèrent en ligne offrent de nouvelles opportunités pour la société civile, mais elles ont aussi accru la possibilité d'attaques asymétriques »* selon l'OTAN[13]. Le concept de guerre hybride est traité dans le cadre de cette analyse. Les publications sur le sujet plaident pour une recherche sur cette appellation de la guerre qui est confirmée dans les déclarations politiques. En revanche, les notions de conflit dans le cyberespace et de cyberattaques sont préférées au terme de cyberguerre, qu'il convient

---

[4] RDIA-008_AS(2012) N° 148/DEF/CICDE/NP du 28 juin 2012 Éléments d'analyse systémique pour la planification opérationnelle.

[5] Les acteurs hybrides vont maintenir leur niveau de violence en dessous du seuil toléré par la communauté internationale afin que leurs actions ne soient pas des « agressions armées » au sens de l'article 51 de la Charte des Nations Unies. Ils paralysent ainsi, sur le plan juridique, toute intervention militaire extérieure.

[6] « […] *cette guerre* [annexion de la Crimée par la Russie et crise en Ukraine en 2014] *n'a pas été déclarée* » selon Reisinger H, et Golts A : *« Russia's Hybrid Warfare : Waging war below the Radar of Traditional Collective Defence »* dans Jacob A, Lasconjarias G, *NATO's Hybrid Flanks, Handling unconventional Warfare in the South and the East*, dans *NATO Research Paper*, N°112, avril 2015, chapitre 7.

[7] RDIA-007_CONFLICTUALITE(2012) du 29 mai 2012, p.13-17-18.

[8] LBDSN 2013, Paris, La documentation française, 2013, p.85.

[9] Gartzke, E.: *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*. International Security, 2013, 38. évfolyam, 2. szám, 41–73. http://belfercenter.ksg.harvard.edu/files/IS3802_pp041-073.pdf

[10] Filiol, E : *The operational reality of « cyberwar » and « cyber attacks » - How to paralyze a country with the cyber* dans www.securiteoff.com/reality-of-cyberwar-how-to-paralyze-the-usa-really/

[11] Yannick Harrel, expert du monde russe et de son proche étranger a étudié à Moscou et à Veliky-Novgorod, puis travaillé à Saint-Petersbourg. Membre de *l'Alliance GéoStratégique* et animateur du blog *Cyberstratégie Est-Ouest*, il est chargé de cours en cyberstratégie économique et financière à Strasbourg.

[12] Bertrand Boyer est Saint-Cyrien, breveté de l'école de Guerre et diplômé de Télécom ParisTech. Il a publié plusieurs articles sur la cyberguerre et la stratégie dont *Cyberstratégie, l'art de la guerre numérique*, Nuvis, 2012.

[13] NATO – 074 CDS 11 E *Information and National Security*.

encore d'utiliser avec prudence. Si le cyberespace peut être comparé à un bien d'intérêt commun[14], cette *Terra Incognita,* ou dernière frontière, peut être mise en valeur. Cette dernière proposition appelle naturellement l'exercice de la propriété privée et de la conquête de ce vide. Une des démarches de cette étude est donc d'esquisser ce que sont ces formats particuliers de guerre et d'établir leurs liens avec l'utilisation des cyberattaques, point pressenti dans certaines publications ayant trait à cette question, mais encore peu souligné et analysé.

La présente analyse se base sur une première approche philologique des concepts et définitions traitant de la guerre hybride, en valorisant le contexte et l'environnement de cette question. Par une approche prospective, l'objectif consiste à apporter les éléments de compréhension de l'hybridité et leur lien avec le domaine de l'information.

La documentation sur laquelle s'appuie cette analyse dresse un état de l'art de la notion de guerre hybride. Dans ce cadre, les sources sont organisées en trois catégories : la première traite de la guerre hybride, la seconde du domaine du cyberespace et de ses potentialités d'affrontements, la troisième évoque les documents de théories ou doctrines nécessaires à une meilleure compréhension des concepts étudiés.

Dans le domaine de la guerre hybride, les différentes sources étudiées reposent sur les recherches américaines des officiers F. Hoffman et B. Fleming au sujet des origines de l'hybridité, sur les publications de la division recherche du centre de doctrine et de concept de l'OTAN sous la direction de G. Lasconjarias, des documents de doctrine OTAN et français ainsi que sur le colloque *« Affronter les nouvelles formes de conflictualités, de nouveaux défis pour les forces terrestres »* du Centre de Doctrine et d'Emploi des Forces (CDEF).

En ce qui concerne le domaine des cyberattaques, les réflexions de Bertrand Boyer[15] et Yannick Harrel[16] permettent d'appréhender ces questions. Ce sont les analyses d'Erick Gartzke[17] qui *a contrario*, relativisant le thème de cyberguerre, laisse entrevoir le lien d'opportunité stratégique entre les cyberattaques et la guerre hybride.

Enfin, un ensemble de documents de tactique et de stratégie générale offre un cadre de compréhension pérenne au profit de cette étude, que conférences et colloques sont venus

[14] Ou *Global Commons,* d'après Olivier Kempf dans *Introduction à la cyberstratégie,* éd. Economica, 2012, p. 41.
[15] Boyer B, *Cybertactique, Conduire la guerre numérique,* éd. Nuvis, 2014
[16] Harrel Y, *La Cyber Stratégie Russe,* éd. Nuvis, 2013
[17] Gartzke E, *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*. *International Security*, 2013, 38. pp. 41-73.

enrichir. Pour une grande partie, les publications otaniennes et américaines sont disponibles en ligne sur les sites dédiés et offrent une pluralité de sources ouvertes pour le chercheur.

Dans le contexte actuel marqué par des affrontements de nature souvent asymétriques, l'adversaire hybride cherche à contourner les puissances classiques, les États et leurs forces armées. Dans ce cadre, ce type de conflit reste difficile à définir. Or, cette difficulté à en apprécier les contours et à en donner un cadre constitue l'essence même de ces conflits. Le postulat de cette analyse repose sur le fait qu'un des piliers de l'hybridité pourrait privilégier l'acquisition de la supériorité informationnelle, dont il convient d'étudier la place et les opportunités qu'elle représente à travers l'usage des cyberattaques.

Cette analyse est ainsi divisée en deux parties. La première est consacrée à la guerre et aux menaces hybrides dans une approche dédiée notamment à l'historiographie liée à ces concepts, la seconde aux cyberattaques et au milieu informationnel.

1. Guerre hybride entre sémantique et définition

1.1 L'origine du terme de guerre hybride

La première apparition du terme d'hybridité est due à l'écrit de deux officiers américains, le général James N. Mattis et le colonel Frank G. Hoffman, publié en 2005[18], même si le contour de ce concept existait déjà sous d'autres appellations, dont celle de « guerre ambiguë », plus prisée des britanniques à l'époque. Or, pour Élie Tenenbaum[19], l'historicité de ce concept est antérieure à l'année 2005, car la thématique des nouvelles conflictualités se pose depuis 25 ans, ce qui témoigne de la pérennité d'un problème non résolu[20]. Sous les libellés de guerre de basse intensité, irrégulière, une opposition se créé face à la guerre dite classique, celle qui oppose les États entre eux. Dès 2006, la guerre entre Israël et le Hezbollah a fourni un cadre pratique à l'hybridité. Depuis 2007 et 2011, Frank Hoffman et Brian Fleming ont développé la réflexion sur ce concept. Il convient dès lors de noter que le *Quadriennal Defense Review* (QDR) américain de 2010 intègre la guerre hybride[21], très influencé par les articles de Frank

[18] Mattis, James N. (*Gen*) et Hoffman, Frank G. (*Col. ret.*), « *Future Warfare: The Rise of Hybrid Wars*, » dans *Proceedings 131, No.11, November 2005*, pp.18-19.
[19] Élie Tennebaum est chercheur au Centre des études de sécurité de l'IFRI et coordinateur du Laboratoire de recherche sur la défense (LRD). Il travaille sur les thématiques des interventions militaires et des opérations extérieures et sur la guerre irrégulière. Il a enseigné la sécurité internationale à Science-Po et l'histoire des relations internationales à l'Université de Lorraine.
[20] Tenenbaum É, actes de la conférence « *piège de l'hybridité* » à l'occasion du colloque *« Affronter les nouvelles formes de conflictualités, de nouveaux défis pour les forces terrestres »* École militaire, 10 février 2016.
[21] *U.S. Department of Defense, Quadriennal Defense Review Report 2010*, Washington DC, février 2010, p. 8.

Hoffman. D'un autre côté, l'OTAN et plus précisément l'*Alliance Command Transformation* (ACT), a initié une réflexion approfondie sur les formes futures des conflits. Élie Tenenbaum observe qu'à la tête d'ACT, sous l'impulsion du Général Mattis (co-rédacteur avec Frank Hoffman du document fondateur portant sur la guerre hybride) l'OTAN débute la réflexion sur ses nouveaux concepts stratégiques en 2010[22]. De son côté, la France, après une première approche doctrinale[23], accepte officiellement le terme de guerre hybride dans son livre blanc sur la défense et la sécurité nationale de 2013[24] et ne cesse d'y recourir dans les discours officiels,[25] depuis les attentats de 2015 à Paris.

Pour Frank Hoffman[26], des concepts précurseurs ont précédé l'avènement de la guerre hybride comme les notions américano-centrées de *New Wars* et *Fourth Generation Warfare (4GW)*, des actions terroristes combinées à celles d'acteurs tiers, dans un contexte flou de crise ou de paix imparfaite, affaiblissent des États entraînant leur désintégration sociale. Il décrit également l'apport des guerres combinées ou composites (*Compound wars*) qui reposent sur l'observation des conflits récents. Historiquement, le combat des partisans appuie l'action des forces régulières. La campagne de Russie de 1812 en constitue un exemple. Pour Élie Tenenbaum, la guerre hybride exprime une polarité entre les modes de conflits réguliers et irréguliers, des concepts introduits entre les XVII^{e} et XX^{e} siècles[27].

Christian Malis[28] voit la guerre hybride comme l'héritière de la guerre couverte de Richelieu, de la stratégie indirecte de Beaufre et de la guerre révolutionnaire de Mao Zedong[29]. La guerre hybride n'est donc pas un phénomène nouveau, car elle s'inspire des guerres passées et en amplifie le domaine d'action.

---

[22] Tenenbaum É, *"Hybrid Warfare in the Strategic Spectrum: An Historical Assessment"* dans Jacob A, Lasconjarias G, *NATO's Hybrid Flanks, Handling unconventionnal Warfare in the South and the East*, in *NATO Research Paper*, N°112, avril 2015

[23] CICDE, RDIA-007_CONFLICTUALITE(2012), 29 mai 2012

[24] LBDSN2013, *op cit.* p.85.

[25] Dans son discours d'ouverture des Assises nationales de la Recherche stratégique 2015 : « qui est l'ennemi ? », le ministre de la Défense Jean-Yves Le Drain affirme : « *Avec Daech, la désignation de l'ennemi ne fait pas de doute. Sa caractérisation […] soulèv(e) en revanche d'autres difficultés, car nous avons affaire à un ennemi profondément hybride* ».

[26] Hoffman F, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac institute for Policy Studies, décembre 2007, p. 18.

[27] Tenenbaum, *op cit.*, p. 99.

[28] Christian Malis, ancien élève de l'école normale supérieure et docteur habilité en histoire contemporaine, entre en 2002 comme responsable de la planification stratégique du *Business Group Communications* de la société Thalès, puis occupe les fonctions de directeur des études stratégiques de la Division des systèmes d'information et de communication sécurisés en 2010. Lieutenant-colonel de réserve, il est professeur associé en histoire militaire et en stratégie aux écoles de Saint-Cyr Coëtquidan et conseiller scientifique du directeur du centre de recherche des écoles de Coëtquidan (CREC).

[29] Malis C, *« Comprendre l'hybridité, la stratégie de contournement »* actes du colloque *« Affronter les nouvelles formes de conflictualités, de nouveaux défis pour les forces terrestres »* École militaire, 10 février 2016

1.2 Définitions du concept

La guerre hybride pose un problème de définition. Il ne semble pas y avoir de consensus clair à ce sujet. Le concept de guerre hybride est initialement un terme anglo-saxon et américano-centré. Les écrits des officiers américains Mattis et Hoffman en assurent une certaine paternité. Selon la définition de L'OTAN[30] : *« La guerre hybride est déterminée par un adversaire actuel ou potentiel, comprenant des acteurs étatiques, non-étatiques et terroristes, possédant la capacité, démontrée ou supposée, d'employer simultanément des moyens conventionnels et non conventionnels, en les adaptant en fonction de leurs objectifs* ». Christian Malis[31] constate que, pour l'OTAN, la guerre hybride possède une *surextension de ses modalités*. Pour Élie Tenenbaum, la guerre hybride se focalise avant tout sur la dualité des modes réguliers et irréguliers. L'OTAN élargit cette vision en y incorporant les visages multiples d'acteurs tiers et non-étatiques qui ont recours à l'influence et au combat irrégulier, lorsque cela présente un avantage pour eux.

En France, la définition du CICDE se distingue peu de celle de l'OTAN : « *une stratégie combinant des actions conventionnelles et non conventionnelles, menées dans les champs les plus divers par des moyens militaires ou non militaires, mis en œuvre par des adversaires étatiques aussi bien que non étatiques* »[32].

L'utilisation d'acteurs tiers, les « *proxies* », dans le conflit hybride, entraîne une complexification de la notion de guerre et tend, selon une lecture rigide de cette règle, à interdire de qualifier de « guerres » ce type de conflits, au risque de ne pas voir venir de tels événements et de s'exposer à une rupture stratégique[33]. Or, le caractère social de la guerre s'impose comme une donnée fondamentale. Le lieutenant-colonel Olivier Entraygues pousse cette réflexion plus loin pour « *placer la pensée stratégique au cœur de toutes les représentations du phénomène guerre, dans ses dimensions sociobiologiques et évolutionnistes*[34] ». La guerre est donc un phénomène sociobiologique car il est avant tout étiologique, selon le lieutenant-colonel Entraygues, qui citant le général J.F.C. Fuller[35], compare la guerre à la maladie dans toute son acception, notamment psychique, exhortant

[30] *NATO Strategic Planning & Concepts*, février 2010.
[31] Malis C, *op cit.*
[32] RDIA-007_CONFLICTUALITE(2012), *op cit.* pp. 13-17-18.
[33] Fleming, *op cit.*, p. 44. L'auteur affirme également : *"In sum, the hybrid threat organization is potentially a revolution in military affairs that will continue to mature in the coming decade. […] military professionals should attempt to step back and assess the environment to determine if they are in the midst of a potential paradigm shift"*.
[34] Entraygues O (LCL), *Formes de guerre, stratégies et déclin de l'Occident*, éd. Economica, novembre 2014, p. 22.
[35] Fuller, J.F.C *Armament and History, Londres*, p. 226.

ainsi à étudier la guerre selon de nouvelles perspectives[36]. Dans la guerre interétatique classique s'exprime une volonté de puissance intelligible. Il en résulte que les détracteurs du concept se refusent à qualifier de guerre ce qui ne fait l'objet d'aucune déclaration préalable et n'oppose pas un État à un autre. Il convient enfin de souligner que le terme de guerre hybride provient de la traduction de l'américain *hybrid warfare* et non *hybrid war.* La distinction entre *war*, « phénomène social », « *une situation dans laquelle deux États ou plus ou des groupes d'individus se combattent durant un certain temps* »[37] et *warfare,* traduisible en méthode de conflit, « *activité de mener une guerre, en particulier en utilisant des armes ou des méthodes particulières* »[38], n'existe pas en français. Or, les essayistes américains se sont gardés d'attribuer à leur « trouvaille », un caractère absolu. Cette caractéristique hybride renvoie à une modalité conflictuelle, un simple visage possible de la guerre.

Un risque induit de cette hésitation sémantique, a pour effet que l'État qui structure et rend légitime l'acte guerrier au titre du *Jus ad Bellum*, ne peut exercer ce droit face à un ennemi flou et désincarné, qui peut refuser de se laisser appréhender. Ce risque accrédite d'emblée le potentiel « disruptif[39] » du concept d'hybridité que relevait le QDR en 2005[40], non en termes technologiques, comme l'indique ce document, mais en termes juridiques tout d'abord. Joseph Henrotin, reprenant en partie une définition de la guerre hybride de F. Hoffman, la décrit ainsi :

> *Tout adversaire qui emploie simultanément et de façon adaptative un mixte de technologies plus ou moins avancées et de modes de guerres irréguliers, y compris le terrorisme, voire des comportements criminels, dans l'espace de bataille afin d'atteindre ses objectifs politiques*[41].

Dans cette acception, une large part est faite à l'aspect criminel et terroriste, ce qui laisse le champ libre à toutes sortes d'acteurs non-étatiques. Nous y reviendrons.

---

[36] Entraygues, *op cit.* p. 15.
[37] *Oxford Advanced Learner's dictionary*, 2000.
[38] *Ibid*. De la même manière dans *Techno-guérilla et guerre hybride, le pire des deux mondes*, éd. Nuvis, octobre 2015, Joseph Henrotin explique : *le concept de « guerre » étant ici à comprendre dans le sens de la traduction anglaise de « warfare », soit « façon de faire la guerre », plutôt que de « war »*. Notes de bas de page, p. 37.
[39] Technologie de rupture (traduction : *Technological breakthrough / Disruptive technology*).
Une « technologie de rupture » est une « technologie » qui permet sur un temps court un saut (percée technologique) dans la valeur opérationnelle (usage, efficacité) et/ou économique des capacités correspondantes. Ce saut peut être induit par une amélioration importante de performance, de coûts, et/ ou de délais. Cette technologie a vocation à remplacer une « technologie » dominante sur un marché, ou à ouvrir de nouvelles fonctions. Commentaire: Une technologie de rupture est, dans la quasi-totalité des cas, non prévisible mais constatée a posteriori; par anticipation, les « technologies émergentes » présentant un fort potentiel de rupture sont parfois qualifiées de «technologies de rupture» dans Guide R-CTI, *Définitions - glossaire des technologies*, DGA, 2014.
[40] *U.S. National Defense strategy of the United States of America, 2005*, pp. 2-4.
[41] Henrotin, *op cit.* p. 44.

1.3 Un concept évolutif et aux prises avec l'actualité

Le concept de guerre hybride évolue en fonction du tropisme national et transnational ; le fait d'appartenir à une alliance comme l'OTAN, dotée d'une réflexion doctrinale, influe sur l'ensemble des membres de l'organisation. Une inflation du terme d'hybridité, véritable concept agglomérant, paraît logique (bien que non souhaitable pour tous ceux qui y sont confrontés) car le poids de l'actualité tend à en compléter constamment la définition. Ceci rend d'autant plus difficile une appréhension juste et limitée de ce concept aujourd'hui.

Un premier constat, à titre de mise en garde, est que le terme de guerre hybride n'est pas employé par leurs auteurs supposés (Le Hezbollah et la Russie parlent respectivement de nouvelle forme de guerre ou d'application de leur doctrine). Il peut également traduire une perception techniciste propre aux États-Unis, bien souvent focalisés sur les capacités « disruptives »[42] et technologiques, plus que doctrinales, de l'adversaire potentiel[43]. Le Colonel(er) Michel Goya apporte une autre explication :

> *Les Américains sont troublés par ce concept [de guerre hybride]. Pour eux la guerre c'est « GO » ou « NO GO ». L'ennemi doit être clairement reconnu et pour les autres conflits, ce sont les « Operations Other Than Wars » (OOTW) pouvant inclure sociétés militaires privées et forces spéciales. Il y a [aux États-Unis] une rigidité de l'emploi de la force.* [44]

Le point de vue de Frank Hoffman sur la guerre hybride repose sur l'évolution progressive des formes de conflictualité vers l'hybridité. Irrégulières et privées par nature, les guerres se sont structurées politiquement du fait de l'implication des États, seuls détenteurs de la force légale. Invoquant les guerres dites de 4ème génération (4GW), Hoffman, reconnaît l'importance du discours niant la pertinence du concept 4GW sur un plan historique. C'est pour cette raison qu'il aborde le concept de guerres composites (*Compound Warfare*), polarisées par l'utilisation des modalités régulières et irrégulières, comme une des bases de la guerre hybride. Remarquant enfin les écrits des officiers de l'armée populaire de libération chinoise au sujet de la guerre hors-limites (*unrestricted warfare*)[45], Hoffman souligne

[42] *Idem* note de bas de page n°38.
[43] Rumsfeld, D : *"**Disruptive** challenges may come from adversaries who develop and use breakthrough technologies to negate current US advantages in key operational domains"* dans *The National Defense strategy of the united States of America, Washington DC, 2005, op cit.* pp. 2-4.
[44] Goya M, interview à l'occasion de la conférence « *L'innovation dans le milieu militaire* », session du comité « Penser Autrement » de l'école de Guerre, 18 février 2016.
[45] Christian Malis, dans son intervention lors du colloque du CDEF « *Affronter les nouvelles formes de conflictualités, de nouveaux défis pour les forces terrestres »* qualifie leur ouvrage de « *véritable bible de la guerre hybride* ».

l'approche visionnaire de cet écrit concernant une appréhension logique et claire des possibilités offertes par la mondialisation.

Plus réservé sur le concept de guerre hybride, Élie Tenenbaum pense raisonnable de se limiter à la dualité régulier-irrégulier pour définir le concept. La vision proposée par Hoffman va en effet plus loin et intègre assez logiquement tous les moyens disponibles pour mener ce genre de conflit. Pour Hoffman, la définition d'Élie Tenenbaum répondrait au seul aspect des *Compound Wars*. Or, Hoffmann fournit une grille de lecture permettant d'identifier la guerre hybride.

- Omni-direction : il n'y a pas de distinction entre les différents « champs de batailles ». Ils se trouvent à la fois sur terre, mer, air, mais aussi dans l'espace, dans les domaines politiques, économiques, culturels et moraux ;
- Synchronisation : les différents champs de batailles génèrent des effets. Ces derniers sont additionnés pour atteindre un effet final recherché. Cet effet est atteint par agrégation simultanée des résultats obtenus sur les différents « champs de batailles » ;
- Asymétrie : le mélange des moyens conventionnels et irréguliers va plus loin encore[46] que dans un conflit de type guerre du Vietnam. Entre le partisan en civil et le militaire en uniforme, il peut y avoir un recours à des « hommes verts » sans insignes d'unité ou grades distinctifs : un autre moyen de « flouter » la distinction entre combattant régulier et irrégulier.

La guerre hybride existe sous des formes complexes et diversifiées. Plusieurs conflits récents peuvent entrer dans la catégorie des guerres hybrides. La première de ces guerres à entrer dans cette catégorisation est la guerre entre Israël et le Hezbollah en 2006. Les combattants de ces guerres nouvelles se servent de moyens sophistiqués : drones de combat, missiles, écoutes de téléphones mobiles. Parallèlement, ces combattants se servent aussi de moyens plus rustiques[47]. Le lieutenant-colonel Entraygues affirme ainsi : « *Face à la modernité, la stratégie occidentale génère l'archaïsme illustré par les petits groupes armés du Hezbollah et de Daech. Ces petits éléments tactiques qui incarnent des armées hybrides, low cost et high tech, développent des stratégies qui perturbent l'action militaire des pays occidentaux. »*[48] Au

[46] Notamment par la mise en œuvre de la « *guerre illimitée* » ou « *hors limite* » selon le traité chinois éponyme des colonels Qiao et Wang de l'Armée de Libération Populaire.
[47] Hoffman : "We can expect to see a lot of tactical plagiarism […] coupled with wild cards or hybrid adaptation where our adversary has learned to use high technology in unique and unanticipated ways", *op. cit.* p. 16.
[48] Entraygues, *op cit.* p. 23.

sujet de la stratégie, certains analystes[49] observent que l'hybridité ne suffit pas pour obtenir des objectifs de ce niveau d'enjeu : « *l'hybridation profite davantage aux armées régulières sur le plan tactique qu'elle ne permet aux organisations irrégulières d'atteindre leurs objectifs politiques* ». Ainsi le *Hezbollah* peut revendiquer l'atteinte d'objectifs tactiques et opératifs comme la victoire contre *Tsahal* ou un contrôle accru sur le Liban, mais en aucun cas « *la destruction de l'État hébreu*[50] » comme objectif stratégique. Ce constat pose la question d'une lecture différentiée de l'hybridité selon les niveaux stratégiques, opératifs et tactiques.

Un domaine particulier devient le champ de bataille de prédilection de l'acteur hybride, il s'agit du domaine de l'information.

2. Guerre hybride et cyberattaques, l'apport du champ informationnel

2.1 Une extrême prégnance informationnelle

Selon Diego A. Ruiz Palmer[51], l'approche Russe de la guerre hybride se concentre sur l'effet d'une « guerre sans contact », où il convient de favoriser une stratégie d'anti-accès sur le théâtre d'opération, physique, voire informationnel. Pour ce dernier, le recours à la sphère cyber est particulièrement encouragé. Les actions qui s'y déroulent tendent à interdire l'accès au cyberespace, empêchant l'adversaire de s'y déployer[52]. Ainsi, l'attaque sur TV5 Monde démontre l'importance de l'information et de son utilisation dans ce cadre, en termes d'influence[53]. Que ce soit pour la Russie ou *Daech*, on constate l'emploi permanent des médias, des réseaux sociaux et de vidéos sur internet. L'Etat ou l'organisation qui utilise la guerre hybride cherche à mettre en œuvre des actions déstabilisantes dans le domaine de l'information en neutralisant les atouts de l'adversaire ou en les utilisant contre lui. La recherche de la supériorité informationnelle est donc une clef du succès dans ce genre de

[49] Taillat S, *Modes de guerre : stratégies irrégulières et stratégies hybrides*, dans Taillat S, Henrotin J, *et ali*. *Guerre et stratégie*, PUF, décembre 2015, p. 268.
[50] *Idem*.
[51] Palmer, Diego A. Ruiz, *Back to the Future? Russia's hybrid Warfare, Revolutions in Military Affairs, and Cold War Comparisons* dans *NATO's Response to Hybrid Threats* by Guillaume Lasconjarias and Jeffrey A. Larsen, p. 49
[52] Sens du territoire éthologique et non politique de Bertrand Boyer dans *Cybertactique, conduire la guerre numérique*, 2014, éd Nuvis, p. 29.
[53] Harbulot C, *La France peut-elle vaincre DAECH sur le terrain de l'information*, École de Guerre économique, Mai 2015. *« Dans l'attaque de TV5, au-delà du niveau de capacité technique des agresseurs, il faut voir un test de neutralisation de l'information impactant toutes les autres télévisions. […]* » p. 6, « *Le piratage de TV5, attribué pour l'instant à Daech, est-il devenu le symbole de la montée en puissance de la guerre de l'information que livrent aujourd'hui des groupes terroristes, des mouvements armés à des États ?* » p. 9

conflit. A ce titre, dans *Introduction à la cyberstratégie*, Olivier Kempf distingue trois couches du cyberespace. La couche physique, où se déploient les infrastructures d'internet, la couche logique, celle du code et des interconnexions au langage machine et la couche sémantique ou informationnelle[54]. C'est dans cette dernière qu'apparaît la dimension sociale du cyberespace, car loin d'être neutre, Olivier Kempf explique que le cyberespace est également ce qu'il véhicule[55], soit l'information porteuse de sens en elle-même et traduisant les interrelations, le lien social entre individus[56]. Les réseaux sociaux en sont la traduction concrète. La doctrine française reconnait également cette dimension sociale du cyberespace[57]. L'information est de plus en plus une donnée clef dans toute forme de conflit, qu'il soit classique ou irrégulier. Ce « *levier puissant de domination du champ de bataille*[58] », lorsqu'il est bien utilisé, permet à la force déployée en territoire d'opération d'être mieux acceptée par les populations locales. Bien intégrée par la communauté militaire, la couche cognitive figure dans les travaux de planification des opérations, caractérisant l'approche globale[59]. L'irruption de l'information comme champ de bataille, en tant que tel, est une nouveauté, une étape supérieure de ce processus d'intégration de l'aspect cognitif des opérations[60]. Quoi qu'il en soit, l'enjeu des conflits (qu'ils soient réguliers ou irréguliers) à dominance informationnelle demeure la population. Les possibilités offertes par la couche sémantique du cyberespace sont également du ressort du décloisonnement de l'information, qui permet à des cellules isolés (activistes ou autre) de diffuser information ou propagande. Les réseaux sociaux sont un moyen privilégié pour remplir cette fonction.

Pour le général de division Parlanti[61], les sociétés actuelles sont dépendantes de l'information. *« La transparence et l'opinion sont aux cœurs des enjeux : il y a un phénomène d'addiction aux infos. […] La comparaison devient raison et tension. La sensibilité des médias influe sur le raisonnement politique. C'est un nouvel ADN de crise. […] La guerre hybride est un concept ancien et une nouvelle « drôle de guerre » mondialisée où la volonté et la vision sont aussi importantes que les capacités. La perception des populations supplante le domaine de*

[54] Kempf, *op cit*. p. 11.
[55] *Ibid*, p. 14.
[56] *Ibid*, p. 13.
[57] Dans la DIA 3.40_CYBER(2014) du 28 mars 2014, reprenant l'analyse d'Olivier Kempf, il est écrit que le cyberespace s'articule notamment sur : « *une zone « sociale », constituée des données et informations de toutes sortes, sous forme numérique, qui se trouvent dans le cyberespace (fichiers, sites, adresses et codes de connexion, …), mais aussi des individus, lesquels peuvent disposer de multiples « identités numériques » (adresses e-mail, pseudonymes, adresses IP, pages sur les réseaux sociaux, blogs, numéros de téléphone, avatars …),* pp. 17-18.
[58] Bertrand B, *op cit*. p. 108.
[59] C.f. note de bas de page n°3.
[60] Bertrand B, *op cit*. p 109.
[61] Parlanti J-F, actes de la conférence *« Guerre hybride : une nouvelle forme d'engagements des forces armées »* à l'occasion du colloque *« Affronter les nouvelles formes de conflictualités, de nouveaux défis pour les forces terrestres »* École militaire, 10 février 2016.

la légalité ». Il est compréhensible que dans un tel contexte, l'acteur de la guerre hybride souhaite obtenir la supériorité informationnelle. Pour le professeur Kate Utting[62], c'est exactement ce que recherche la Russie dans son approche doctrinale actuelle des conflits. En réaction à cette perception Russe de l'influence et de l'information, cette nécessité d'obtenir la supériorité informationnelle, avant même la puissance militaire, est soulignée dans un document[63] de l'OTAN analysant la crise ukrainienne. Cette supériorité informationnelle est toutefois plus difficile à obtenir face à des adversaires confondus avec les usagers de l'internet, qui savent parfois faire preuve d'une inventivité et de connaissances poussées dans le domaine numérique.

2.2 Entre technologies duales[64] et TIC[65]

Une des caractéristiques de ce début de XXI[e] siècle est la multiplicité des acteurs dans le domaine de l'information en raison de l'internet qui a démocratisé l'usage de la communication et, par conséquent, des outils d'influence. L'internaute se fait ainsi le relai conscient ou inconscient des actes politiques des acteurs étatiques comme des revendications des acteurs non-étatiques. Les réseaux sociaux en constituent un exemple évident, tant ils sont devenus des outils de campagne d'information, de recueil de renseignement, de levier de recrutement, de désinformation, de propagande, voire de levée de fonds dans certains cas. Toutes ces possibilités offrent une source inépuisable d'outils abordables pour l'acteur hybride. La possibilité de diffuser gratuitement du contenu ou des liens hypertextes soutenant une cause particulière constitue une opportunité non-négligeable que les parties en présence saisissent. Dans le cas de la crise russo-ukrainienne de 2014, les activistes pro-russes ont pu forger des récits accusant les forces gouvernementales de répression et de perte de contrôle de leurs forces de sécurité[66]. Des profils *Twitter ad hoc* ont généré une intense toile médiatique que les forces gouvernementales ukrainiennes ont eu du mal à contrer tant les soutiens pro-russes ont affiché un profil uni. Les autorités Russes ont bénéficié d'un soutien très important

[62] Utting K, conférence *"Influence" Advanced Command and Staff Course, Shrivenham*, 24 février 2016.
[63] *NATO StratCom Centre of Excellence, Analysis of Russia's information campaign against Ukraine*, 2014
[64] *Une « technologie duale » est une « technologie » qui présente un double usage avéré ou pressenti à la fois civil et militaire, en anglais : « Dual use Technologies »* dans Guide R-CTI, *Définitions - glossaire des technologies*, DGA, 2014.
[65] Les TIC sont définies dans la DIA 3.40_CYBER(2014) Cyberdéfense n° 82/DEF/CICDE/DR du 28 mars 2014 comme le « *terme qui regroupe les techniques utilisées dans le traitement, le stockage et la transmission des informations. Elles sont principalement liées à l'informatique, aux réseaux, dont Internet, et aux télécommunications* », p. 18.
[66] Les histoires forgées de toutes pièces du médecin d'Odessa et de la femme enceinte étranglée sont deux exemples parmi d'autres cités dans *NATO StratCom Centre of Excellence, Analysis of Russia's information campaign against Ukraine*, 2014, *op cit.* p. 30.

et d'une influence très forte sur *Twitter* contrairement aux organes gouvernementaux ukrainiens et aux membres de l'Union Européenne.

Toutes ces possibilités induites par les technologies de l'information et des communications (TIC), centrées sur internet, ne sont pas les seules opportunités pour un adversaire irrégulier de mettre en difficulté des forces conventionnelles. Le détournement des technologies duales, pouvant impliquer un usage tant militaire que civil demeure une opportunité. L'usage de la téléphonie mobile pour déclencher des engins explosifs improvisés, l'utilisation de drones par le *Hezbollah* et *Daech*, le guidage des tirs d'artillerie et de roquettes via une application comme *Google Earth* et par l'emploi du GPS, constituent quelques exemples des nombreux usages inattendus d'outils mis à la disposition du monde civil et donc de tout adversaire irrégulier ou hybride. Cette facilité à détourner la technologie, habituellement réservée aux nations occidentales, par des « insurgés innovants » a été soulignée dans l'ouvrage de Balencie et de La Grange : *Les guerres bâtardes : comment l'Occident perd les batailles du XXIe siècle.* Dans ce qui constitue la force d'une nation comme les États-Unis, la puissance technologique, réside également une faiblesse intrinsèque que peuvent exploiter avec succès les adversaires irréguliers. Si dans le cadre de l'affrontement asymétrique, les États rencontrent des difficultés, il convient de s'interroger sur le danger que représente un adversaire hybride rompu à la guerre de l'information et maîtrisant des moyens à moindre coût à sa disposition. A ce titre, le cyberespace, source de tous les espoirs et vecteur de progrès, à la portée de tous types d'acteurs, constitue également le talon d'Achille des organisations internationales comme des États. La définition de la guerre hybride de J. Henrotin[67], mentionne « *le terrorisme, voire des comportements criminels »* mis en œuvre sur le champ de bataille. Ce champ de bataille comprend à présent la dimension du cyberespace. Les criminels qui y prospèrent disposent donc d'un lieu propice à la fois à l'exercice de la violence et comme une base arrière.

2.3 Le cyberespace, potentiel de conflictualité

Le mot *cyber*, qui provient de la notion initiale de cybernétique, ou science de gouverner aux systèmes humains, a retrouvé de nombreuses déclinaisons au fil des intérêts et menaces provenant des systèmes d'information[68]. Dans l'acception russe du terme, le cyberespace devient un enjeu culturel et de survie de leur civilisation, là où les Américains, insistent sur

[67] Cf.1.2 et notes de bas de page n°38.

[68] Kempf : « *En effet, le préfixe cyber est utilisé à profusion et à toutes les sauces : cyber-café, cyber-avocat … et dans le domaine de la sécurité : cybersécurité, cyberdéfense, cyberattaque, cyber Pearl Harbor* », *op cit*. p. 5.

l'aspect technologique de la question. Yannick Harrel souligne la vision russe du cyberespace, marquée par l'effondrement de civilisation qu'a constitué la perte de la *Rus' de Kiev*[69] en 1240, puis les invasions successives en provenance d'Europe, faisant de la Russie une forteresse assiégée[70]. En modelant profondément les ressorts de la pensée Russe, militant pour un besoin fort en service de renseignement, ce traumatisme initial a lié la stratégie cyber de ce pays à la perception d'une condition de survie de la civilisation slave dans son ensemble. La rhétorique pro-russe lors de la crise ukrainienne n'a pas manqué de rappeler cet état de fait en maintes occasions[71].

Dans son approche du cyberespace[72], Olivier Kempf distingue les sphères physiques et connues que sont les sphères terrestres, maritimes, aériennes puis spatiales, de la sphère virtuelle du cyberespace. Vu comme *Terra Incognita* ou *Terra nullius*, ce dernier espace est un espace à conquérir, un espace de prédation et donc de forte conflictualité. La cybercriminalité qui s'y exerce fait l'objet d'un intérêt croissant de la part des États qui cherchent à s'en prémunir, mais aussi de la part de terroristes, d'activistes et d'autres cellules pouvant être employés par d'autres États ou organisations moins scrupuleux. Pour ces derniers, les cybercriminels permettent d'accéder à des ressources et informations utiles pour servir leur cause (commerce, monnaie d'échange, renseignement d'intérêt économique ou militaire). Dans le cas d'un recours à des *Hackeurs Black Hats*[73], ces acteurs peu scrupuleux bénéficient d'un renfort discret car les cyberattaques sont difficilement imputables à qui que ce soit. *Daech* aurait ainsi sous-traité à un groupe de *Hackeurs* son attaque contre TV5 Monde afin de mener une opération d'influence très spectaculaire[74]. Les pirates informatiques peuvent à l'occasion passer pour de fervents patriotes une fois leur mission réussie[75]. Le cyberespace est donc un espace de non-droit, où les règles du droit international peinent à

[69] État féodal regroupant les peuples slaves de l'est et des populations Varègues, autour de Kiev, sa capitale.
[70] Harrel Y, *La Cyber Stratégie Russe*, Nuvis, 2013, 245 p., pp. 47-48-49.
[71] Le NATO *StratCom Centre of Excellence, Analysis of Russia's information campaign against Ukraine*, 2014 cite le discours du patriarche Orthodoxe Kirill, utilisant les termes de « *monde Russe* » et « *pays du monde Russe* », p. 22. Le discours du président Russe V. Poutine aux diplomates russe le 2 juillet 2014 a également résumé les préoccupations liées à la Crimée « *terre de la gloire militaire Russe* ».
[72] Kempf, *op cit*. p. 13.
[73] *Les Black Hats* sont les pirates qui agissent pour leur compte et opérent illégalement en fonction d'un intérêt financier ou pour leur réputation. A l'opposé, les *White Hats* disposent généralement d'un code éthique et recherchent les failles systèmes pour en avertir les entreprises ou organisations et rendre internet plus sûr. Voir à ce sujet l'article de Berthier Thierry, *Hacktivisme : vers une complexification des cyberattaques*, dans Revue Défense Nationale portant sur *Cyberdéfense et cyberguerre*, novembre 2015, p. 45.
[74] Harbulot C, *op cit.*
[75] Lors des attaques en déni de service (DDOS) subies par l'Estonie, des *hackeurs* Russes avaient réagi au déboulonnage de la statue d'un soldat soviétique à Tallinn en menant ces attaques par patriotisme, selon leurs déclarations. Le gouvernement Russe a nié être l'instigateur de ces attaques. Cf. : Boyer B, op cit. pp. 72-73. Olivier Kempf déclare que la cyberstratégie chinoise *« envisage l'utilisation de hackers patriotes lorsque c'est nécessaire ». Op cit* p. 150.

s'appliquer, un « *Global commons*[76] ». Comme pour le droit de la mer, une certaine prise de position d'acteurs dominants sur la scène cyber pourrait être cristallisée par la mise en place tardive de règlements internationaux. L'enjeu de ces prises de position s'exerce avant tout dans la sphère physique où les infrastructures de l'internet (routeurs, serveurs) font l'objet de luttes de multinationales entre-elles. L'implication des États y est loin d'être neutre. Ainsi, la Russie et la France s'interrogent par exemple sur l'opportunité de laisser des entreprises Chinoises dominer ces secteurs, car elles favorisent le risque de fuite d'informations d'intérêt stratégique et économique[77]. La volonté des États est donc de disposer d'autant d'atouts que possible dans le domaine des infrastructures physiques du cyberespace, permettant de façon couverte, de mettre à leur disposition des données numériques dont disposent les multinationales d'internet, comme *Google* et *Microsoft*. L'affaire *Prism* démontre la possibilité pour les services de renseignement (comme la *National Security Agency*) d'exfiltrer des données des serveurs de ces prestataires de service, en y installant parfois des logiciels espions ou en exploitant des vulnérabilités.

Se dirige-t-on pour autant vers une « cyberguerre » dont les enjeux seraient cantonnés à la domination du cyberespace ? Il est permis d'en douter à plusieurs titres. Tout d'abord cet enjeu repose autant sur les couches virtuelles ou logiques[78] du cyberespace que sur les couches physiques où reposent les infrastructures d'internet comme nous l'avons vu précédemment. Cette perméabilité des milieux impose la prudence sur le choix du terme « cyberguerre » que les écrits de J. Arquilla et D. Ronfeld[79] mettent en lumière. Opérant la distinction entre *netwar* et *cyberwar*[80], les deux auteurs décrivent en revanche les actes des acteurs de la première, approche *softpower* de la « cyberguerre » s'il en est :

> *La plupart des guerres réseaux-centrées seront de nature non-violentes, mais dans le pire des cas, certaines pourraient combiner leurs potentialités, créant un scénario néfaste de conflit de basse-intensité. C'est ce que redoute Van Creveld : « Dans les guerres futures, les guerres ne seront plus menées par des armées mais par des*

[76] Le CICDE dans la RDIA-007_CONFLICTUALITE(2012), en donne la définition suivante, particulièrement intéressante eu égard au potentiel de captation de ces espaces : *« Les Global Commons sont généralement entendus comme les espaces d'usage commun ou collectif, de plus en plus interconnectés, sur lesquels ne s'exerce aucune souveraineté nationale […] » Op cit.* p. 22.

[77] Bockel, J-M, *Rapport d'information sur la cyberdéfense*, Sénat, 18 juillet 2012, p. 117. Ce rapport appelle à interdire sur le territoire européen les routeurs de cœur de réseaux sensibles d'origine chinoise et notamment ceux des entreprises *Huawei* et *ZTE*.

[78] Kempf : « *cette couche peut être assimilée au « software » […] ce qu'on désignera mieux en français en disant qu'elle est logicielle* », *op cit.* p.12.

[79] Arquilla J, Ronfeld D, "*Cyberwar is Coming!*" *Comparative Strategy*, Vol 12, No. 2, 1993.

[80] *"We offer a distinction between what we call "netwar"—societal-level ideational conflicts waged in part through internetted modes of communication—and "cyberwar" at the military level". Ibid*, p. 27.

groupes que nous qualifierions actuellement de terroristes, de guérillas, de bandits et de voleurs, mais qui se présenteraient sous des titres plus honorables[81] *».*

A ce stade, ces deux auteurs décrivent le caractère irrégulier des *« netwarriors »,* avant de poursuivre sur une description très intéressante pour notre sujet :

> *Les secteurs stratégiques [militaires] comprennent la prolifération nucléaire, le trafic de drogue et l'anti-terrorisme, en raison des menaces potentielles qu'ils posent à l'ordre international et aux intérêts de sécurité nationale. De plus, les tendances sociétales plus larges (par exemple, la redéfinition des concepts de sécurité, le rôle nouveau joué par les groupes de pression, la confusion des frontières traditionnelles entre le domaine militaire et non militaire, le public et le privé, ce qui est du ressort de l'État et de la société) peuvent engager les intérêts d'au moins quelques officines militaires dans certaines activités liées aux guerres réseaux-centrées.*[82]

Le recours à l'acte criminel ou terroriste, l'aspect social, dans son acception large, de la conflictualité peut entrainer l'usage de la force militaire conventionnelle dans ce genre de conflit, ce qui implique donc une possible escalade progressive vers un mode plus coercitif : une guerre. Dans leur description du "*cyberwar*", Arquilla et Ronsfeld décrivent une cyberguerre militaro-centrée, penchée sur l'aspect organisationnel des moyens de commandement militaires, qui indique une volonté de confirmer l'importance de l'empreinte au sol des forces armées américaines. Cette perception est techno-centrée, même si les auteurs expliquent que cette *cyberwar* peut se faire en mode « *low-tech* »[83]. Prenant l'exemple de la guerre du Vietnam, les auteurs expliquent la victoire de la *netwar* vietnamienne sur la *cyberwar* américaine[84]. Cette *netwar* s'apparente donc à la conflictualité informationnelle, dans cet essai. De façon très intéressante, les auteurs tirent la conclusion suivante :

---

[81] *Ibid*, p. 29. *"Most netwars will probably be non-violent, but in the worst of cases one could combine the possibilities into some mean low-intensity conflict scenarios. Van Creveld (1991: 197) does this when he worries that "In the future war, war will not be waged by armies but by groups whom today we call terrorists, guerrillas, bandits and robbers, but who will undoubtedly hit on more formal titles to describe themselves."[Traduction de l'auteur].*

[82] *Idem. "Candidate issue areas include nuclear proliferation, drug smuggling, and anti-terrorism because of the potential threats they pose to international order and national security interests. Moreover, broader societal trends—e.g., the redefinition of security concepts, the new roles of advocacy groups, the blurring of the traditional boundaries between what is military and what non-military, between what is public and what private, and between what pertains to the state and what to society— may engage the interests of at least some military offices in some netwar-related activities".[Traduction de l'auteur]*

[83] *Ibid*, p. 32.

[84] *Ibid*, p. 39.

Une leçon : les institutions peuvent être vaincues par des réseaux. Il faut des réseaux pour contrer des réseaux. L'avenir peut appartenir à celui qui maîtrise la forme en réseaux[85].

Pour Éric Filiol, le terme de cyberguerre est impropre[86]. Il suffit en réalité de causer une rupture d'approvisionnement énergique, soit une action tactique, sur des points particuliers d'infrastructure à l'aide de quelques cyberattaques très ciblées[87] et relativement simples à mettre en œuvre.

Erick Gartzke doute de l'efficacité des seules cyberattaques comme pouvant durablement infliger des dommages importants à des infrastructures. En revanche, en affirmant que ces cyberattaques ne peuvent constituer un événement décisif, mais comme complément de moyens plus larges, la notion de guerre hybride refait surface[88].

Conclusion

Concept agglomérant et flou, la guerre hybride est devenue incontournable dans les discours et analyses actuels. Une des manifestations de ce modèle de guerre est de faire du domaine de l'information le champ de bataille principal. Les événements récents, dont la crise ukrainienne, ont révélé la collusion entre les usages de la sphère informationnelle en général, et les cyberattaques en particulier, dans une modalité de conflit totale, sans limites, incarnée par la guerre hybride. Les techniques de déni d'accès dans le cyberespace[89] sont compatibles avec les techniques d'anti-accès[90] terrestres, maritimes et aériennes, qu'elles proviennent de l'expression d'un art opératif, ou d'avancées techniques récentes (missiles de croisière[91]). Sans être uniquement techno-centrées, car elles s'expriment aux moyens d'acteurs irréguliers et rustiques, les guerres et menaces hybrides s'entendent principalement au niveau opératif.

---

[85] *Ibid*, p. 40. "*The lesson: Institutions can be defeated by networks. It may take networks to counter networks. The future may belong to whoever masters the network form.*"

[86] Filiol É, « *cyberguerre: l'arme fatale* » documentaire présenté à l'École militaire, 10 décembre 2015

[87] Filiol É, *The operational reality of « cyberwar » and « cyber attacks » - How to paralyze a country with the cyber.* www.securiteoff.com/reality-of-cyberwar-how-to-paralyze-the-usa-really/

[88] Gartzke : "*It is another to ensure that the damage inflicted translates into a lasting shift in the balance of national power or resolve. Cyberattacks are unlikely to prove particularly potent in grand strategic terms unless they can impose substantial, durable harm on an adversary. In many, perhaps most, circumstances, this will occur only if cyberwar is accompanied by terrestrial military force or other actions designed to capitalize on any temporary incapacity achieved via the internet*". *Op cit.* p. 43.

[89] Cf. 2.1 note de bas de page n°47

[90] Joseph Henrotin cite le cas chinois : « *La stratégie navale d'interdiction d'accès chinoise repose ainsi sur des bombardiers lanceurs de missiles antinavires, […] et de missiles antinavires balistiques guidés sur la base d'informations recueillies aussi bien par des satellites que par des pêcheurs* ». *Op cit.* p. 49. On reconnaîtra ici le caractère asymétrique de la désignation des cibles, le « *low-tech* » côtoie le « *high-tech* ».

[91] Quant aux Russes, le développement et l'expérimentation de missiles de croisières vient récemment renforcer cette tendance à une continentalisation de leur défense opérative.

Poursuivant des objectifs stratégiques de plus ou moins longs termes, l'acteur hybride génère plusieurs fronts, plusieurs opérations, selon la définition d'omni-direction de Hoffman, pour créer les conditions d'un véritable encerclement opératif. A ce stade, l'intention stratégique est encore perçue comme floue ou irrationnelle : les objectifs de long terme de la Russie sont difficiles à déterminer. Le niveau tactique, du point de vue de celui qui fait les frais d'une guerre hybride, est, quant à lui, insuffisant pour appréhender les manifestations hybrides dans leur globalité : s'efforcer de saisir et d'analyser les actions dans le domaine de l'information et du cyberespace au prisme de la seule situation tactique relève de la gageure. Les acteurs de cette conflictualité conservent en outre la possibilité de ménager un flou juridique pour perpétrer leur action dans une relative impunité[92].

Les cyberattaques complètent ainsi la palette de l'hybridité, en particulier dans le domaine de la perception, et en démultiplient les effets. Tout adversaire pratiquant de nouvelles formes de conflictualité dispose, dans le cyberespace, d'un nouvel outil « *disruptif*[93] » pour reprendre les termes du *Quadriennal Defense Review* américain de 2005[94]. En se servant des technologies duales et des TIC, l'adversaire hybride est potentiellement capable de rebattre les cartes des outils de puissance, traditionnellement aux mains des États, particulièrement ceux respectueux du droit international. Dans cette perspective, les cyberattaques constituent une arme d'emploi par excellence et un avantage majeur pour les acteurs de l'hybridité, comme visages probables des conflits futurs.

[92] D'autres acteurs hybrides peuvent ne pas choisir cette option : *Daech* déclare ouvertement être en guerre contre la France. Cette « option ouverte » peut être plus difficile à mettre en œuvre pour un État reconnu sur la scène internationale.
[93] Cf.1.3 notes de bas de page n°39 et 40.
[94] *U.S. National Defense strategy of the United States of America, 2005. Op cit.* pp. 2-4.

Bibliographie :

Ouvrages, articles et revues

A. Guerre et menaces hybrides :

- Entraygues, O (LCL), *Formes de guerre, stratégies et déclin de l'Occident,* éd. Économica, novembre 2014
- Fleming, Brian P. (Major), *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art, School of Advanced Military Studies,* 2011
- *Government Accountability Office* GAO 10-1036R, 2010
- Henrotin J, *Techno-guérilla et guerre hybride, le pire des deux mondes*, éd. Nuvis, octobre 2015
- Hoffman Franck G, *Conflict in the 21st Century: The Rise of Hybrid Wars,* Potomac institute for Policy Studies, décembre 2007
- Jacob A, Lasconjarias G, *NATO's Hybrid Flanks, Handling unconventionnal Warfare in the South and the East*, in *NATO Research Paper*, N°112, avril 2015
- Lasconjarias G, Larsen A, *NATO's Response to Hybrid Threats*, in *NATO Defense College Forum Paper*, 2015
- Qiao L, Wang X, *La guerre hors limites,* trad. Denès H., Paris, rivages poche, 2006
- Taillat S, Henrotin J, *et al. Guerre et stratégie,* PUF, décembre 2015
- *U.S. Department of Defense, Quadriennal Defense Review Report 2005,* Washington DC, 2005
- *U.S. Department of Defense, Quadriennal Defense Review Report 2010,* Washington DC, février 2010

B. Guerre de l'information, cyberattaques :

- Arquilla J, Ronfeld D, *Cyberwar is Coming!* dans *Comparative Strategy*, Vol 12, No. 2, 1993.
- Berthier T, *Hacktivisme : vers une complexification des cyberattaques,* dans Revue Défense Nationale portant sur *Cyberdéfense et cyberguerre*, novembre 2015, p. 45.

- Bockel J-M, *Rapport d'information sur la cyberdéfense*, Sénat, 18 juillet 2012
- Boyer B, *Cybertactique, Conduire la guerre numérique,* éd. Nuvis, 2014
- *Cost of Data Breach Study 2015,* Ponemon Institute
- Filiol E, *The operational reality of « cyberwar » and « cyber attacks » - How to paralyze a country with the cyber.*
- Gartzke E., *The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth*. International Security, 2013, p. 38.
- Harbulot C, *La France peut-elle vaincre DAECH sur le terrain de l'information,* École de Guerre économique, mai 2015
- Harrel Y, *La Cyber Stratégie Russe*, éd. Nuvis, 2013, 245 p.
- Kempf O, *Introduction à la Cyberstratégie*, éd. Économica, 2012
- *NATO StratCom Centre of Excellence, Analysis of Russia's information campaign against Ukraine,* 2014
- *NATO Strategic Planning & Concepts,* février 2010

C. Tactique, art de la guerre et documents de doctrine :

- DIA 3.40_CYBER(2014) du 28 mars 2014
- FT-02 Tactique Générale
- Hubin G (G2S), *Perspectives Tactiques*, Économica, 2000
- NATO – 074 CDS 11 E *Information and National Security*
- Ramel F, Holeindre J-V, *La fin des Guerres Majeures*, Économica, juin 2010
- RDIA-007_CONFLICTUALITÉ(2012) du 29 mai 2012
- RDIA-008_AS(2012) *Éléments d'analyse systémique pour la planification opérationnelle*, 28 juin 2012.
- Warden J, *Enemy as a system*, dans *Airpower Journal*, 1995

Sites internet

- dedefensa.org consulté le 12 avril 2016 ;
- http://belfercenter.ksg.harvard.edu consulté le 23 septembre 2015 ;

- Schadlow N, *The Problem with Hybrid Warfare,* dans *War on the rocks,* http://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/ ;
- ultimaratio-blog.org : Hémez R, *Guy Brossolet ou la dissolution de la pensée dominante*, consulté le 5 avril 2016 ;
- www.securiteoff.com/reality-of-cyberwar-how-to-paralyze-the-usa-really/ consulté le 12 février 2016 ;
- http://warontherocks.com/2015/04/the-problem-with-hybrid-warfare/ consulté le 13 avril 2016 ;
- http://tempsreel.nouvelobs.com/tech/20150409.OBS6741/tv5-monde-ce-que-l-on-sait-de-lacyberattaque.html consulté le 14 avril 2016 ;
- Henrotin J, *Les adaptations de la guerre irrégulière aux nouvelles conditions technologiques : vers la techno-guérilla*, Stratégique 1/2009 (N° 93-94-95-96), pp. 533-566. www.cairn.info/revue-strategique-2009-1-page-533.htm. Consulté le 25 mai 2016.

Interview

- Goya M, COL(er) : « *L'innovation dans le milieu militaire* », conférence du comité « Penser Autrement » de l'école de Guerre, 18 février 2016.

Conférences et colloques

- Coustillère A (VA), *« Cyberguerre : l'arme fatale? »* École militaire, 10 décembre 2015
- Utting K, *« Influence » Advanced Command and Staff Course*, Shrivenham, Royaume-Uni, 24 février 2014
- Actes du colloque *« Affronter les nouvelles formes de conflictualités, de nouveaux défis pour les forces terrestres »*, Centre de Doctrine et d'Emploi des Forces, École militaire, 10 février 2016