ECOLE DE GUERRE

PROMOTION *VERDUN*

2015 - 2016

LA CYBER-HYBRIDITE

Un renouveau majeur dans le système international moderne?

Chef de Bataillon Jean-Charles Coste

Sous la direction du

Colonel Jérôme Pellistrandi

Rédacteur en chef de la revue de la défense nationale

Contenu

Depuis la fin du siècle dernier notre société vie une numérisation exponentielle. Aujourd'hui, à la veille de l'internet des objets, la grande majorité de la population mondiale dispose d'un accès à internet souvent grâce à la téléphonie mobile. Les armées modernes, et au travers elles, leurs Etats, se sont pleinement engagées dans ce nouveau champ de bataille qu'est le cyberespace dans le prolongement du phénomène de "révolution technologique dans les affaires militaires". Parallèlement à cette évolution, le caractère novateur du système internationale a généré une réelle évolution de la conflictualité entre les Etats aujourd'hui qualifiée de "guerre hybride". La présente étude vise donc à évaluer le rôle que joue le Cyber dans cette nouvelle conflictualité au travers de l'étude du concept de "Cyber-hybridité".

Since the end of the last century, our society has mutated in an exponential use of information systems. Today, on the eve of the internet of things, most of the world population is using internet most of the time through mobile phones. Modern armed forces, on behalf of their States, are fully committed to the new cyber battle-space, as an extension of its ongoing Revolution in Military Affairs". Simultaneously; the current international system has generated a modern form of warfare between States, which seems to be new, known as "Hybrid-Warfare". The aim of this study is to assess the key role of Cyber-operations in this apparently new form of warfare, through the analysis of the "Cyber-Hybridity" concept.

LA CYBER-HYBRIDITE

Introduction

Les armées occidentales modernes, dans le prolongement de la seconde guerre mondiale, se sont formées durant des années pour affronter les forces du bloc soviétique dans un conflit dit « conventionnel ». Cherchant à théoriser la guerre pour répondre à des schémas doctrinaux connus, elles se sont orientées vers une forme de réponse presque mathématique. Pourtant confrontées à des conflits asymétriques (Irak, Afghanistan…), elles ont perdu de vue que la guerre n'est que le prolongement de la politique par d'autres moyens[1], et que soumettre l'ennemi sans croiser le fer, « voilà le fin des fins »[2]. En parallèle, nos sociétés se sont numérisées, poussant les forces armées à investir ce nouvel espace de confrontation. Dans ce nouveau contexte, les forces russes ont mené à deux reprises, en Géorgie (en 2008) puis en Crimée (en 2014) des opérations dans un cadre juridique et environnemental complexifié, mettant en œuvre une stratégie en apparence novatrice. Bénéficiant d'un contexte insurrectionnel favorable, ces engagements nécessitent une réflexion actualisée. Aujourd'hui, le sort tant de l'Ossétie du Sud que de la Crimée semble définitivement scellé, et ce malgré une contestation tant interne que de la communauté internationale. En effet, dans ces deux crises, les opérations militaires ont réussi dès leurs premières phases. Au-delà de la supériorité numérique écrasante, c'est bien évidemment la manœuvre russe, combinant des actions à la fois sur le terrain mais également dans le champ des perceptions, diplomatique, et en particulier dans le cyberespace, qui explique ces réussites. Cette « nouvelle » forme de conflictualité a été théorisée sous l'appellation de « guerre hybride »[3]. Elle n'est pourtant pas nouvelle, mais les possibilités offertes par l'utilisation du cyberespace, d'une part, et l'évolution du système international, d'autre part, expliquent ce renouveau.

Si cette stratégie n'est pas à proprement parler novatrice, elle rentre par le biais du cyberespace dans une nouvelle ère. En effet, l'action dans le domaine cyber offre, à la fois aux grandes Nations et, à la fois, aux groupuscules terroristes, une nouvelle dynamique dans

[1] Karl von Clausewitz, De la guerre, p. 703.
[2] *« Etre victorieux dans tous les combats n'est pas le fin du fin ; soumettre l'ennemi sans croiser le fer, voilà le fin du fin. »* (Sun Tzu, *L'art de la guerre*, chapitre 3).
[3] L'intervention russe en Crimée a généré un important débat au sein de l'OTAN sur ce qualificatif d'hybride.

un système international qui reste figé par la dissuasion nucléaire. Ainsi est-il aujourd'hui permis de s'interroger sur la notion même de « cyber-hybridité » tant les cyber-opérations sont aujourd'hui intimement liées à cette forme de conflictualité en plein renouveau qui se caractérise principalement par son aspect dual[4].

Depuis le début des années 2000 de nombreux écrits ont tenté de conceptualiser les opérations dans le cyberespace ainsi que la guerre hybride. La présente étude vise donc à clarifier le lien entre ces deux concepts largement interdépendants au regard des dernières opérations. Toute étude sur ce domaine se heurte, nouvelle analogie avec la dissuasion nucléaire, à la protection du secret. Ainsi, est-il nécessaire de conserver la plus grande réserve sur les écrits relatifs à ces opérations où se mêlent désinformation, opérations secrètes, amplifiées par le flou lié par l'utilisation du cyberespace. La majeure partie des sources citées proviennent donc essentiellement des milieux universitaires, institutionnels et de journaux reconnus. Certains lecteurs s'interrogeront également sur cette notion même de « cyber-hybridité », n'est-elle pas tout simplement juste une forme d'emploi des capacités Cyber ? Nous verrons tout au long de cette étude que si les grandes nations fourbissent leur capacité cyber depuis le début des années 2000, leur mise en œuvre a toujours été limitée à un emploi sous une forme « hybride » proche des « opérations spéciales ».

Cette « Cyber-hybridité » est aujourd'hui un élément clé des relations internationales, car elle offre une dialectique des volontés[5] compatible avec le système international qui limite le risque de montée aux extrêmes dans un monde toujours sous la menace nucléaire. Cette nouvelle forme de « frappes préventives » permet de maintenir une forme réelle de pression, tout en conservant un flou compatible avec le dialogue international. Cette opportunité, intrinsèquement liée à la non-létalité directe des actions cyber et l'impossibilité d'attribuer avec certitude une action, restera vraie dans la limite d'une première action létale qui pourrait générer un nouveau paradigme.

La première partie de cette étude est consacrée à la notion même d'hybridité, aujourd'hui controversée et au lien étroit qu'elle entretient avec le Cyber. Nous étudierons pourquoi ce lien est aujourd'hui une des raisons essentielles au renouveau de cette notion et comment nous emmène-t-il à penser la "cyber-hybridité". Fort de ce caractère actuel, nous

[4] Le terme dual est ici utilisé pour souligner l'emploi de capacités principalement civiles dans le cadre d'opérations militaires.

[5] "Art de la dialectique des volontés employant la force pour résoudre leur conflit" Général André BEAUFRE, Introduction à la stratégie, p121.

repositionnerons le rôle et la fonction du Cyber dans cette nouvelle conflictualité avant d'en définir les contours, son lien étroit avec la guerre électronique, notamment au travers de l'étude des différentes approches que l'on voit aujourd'hui se dessiner sur la scène internationale.

I. Réalité de la cyber-hybridité et place dans le système international actuel,

a. Le concept de la « guerre hybride » qui recouvre deux facettes distinctes

i. Au niveau tactico-opératif : une forme de guérilla qui enchaîne action conventionnelle et non-conventionnelle.

Avant tout, qu'est-ce que la guerre hybride ? Le terme même de guerre hybride fait aujourd'hui controverse. Certains y voient une nouvelle forme de stratégie qui utiliserait l'ensemble du champ des possibles. D'autres encore y voient au niveau tactique une forme de guerre alliant succession d'actions conventionnelles et non-conventionnelles[6]. Si au niveau tactique elle se limite à une succession de raids, d'embuscades et de retraites, elle ne trouve son efficacité que dans sa continuité au niveau opératif voire politique. Au niveau opératif, cette forme de stratégie est complémentaire des formes plus régulières en offrant notamment, dans une logique de *supporting/supported* avec les forces locales, une opportunité intéressante, pour réduire l'empreinte et les conséquences de la présence d'une force étrangère, notamment dans le cadre d'un conflit insurrectionnel[7]. A titre d'exemple, les actions majeures sont alors menées par des forces locales, éventuellement conseillées, alors que les forces étrangères ne réalisent que des actions d'appui ou sur les arrières. Cette forme de stratégie, n'est pas sans rappeler les opérations « occidentales » les plus récentes comme l'actuelle opération *Inherent Resolve* en Irak et en Syrie. Ce type de stratégie n'est pas sans rappelée celle employée par Jules César lors de la conquête de la Gaule.

ii. Au niveau stratégique, la guerre hybride vise l'érosion du soutien de la population par le biais d'une approche indirecte.

La seconde caractéristique est d'agir directement sur les cibles visées par ces conflits. Conformément la notion de seuil que nous verrons ultérieurement(voir infra 1.d), ces actions doivent cibler des objectifs suffisamment périphériques pour ne pas pousser l'adversaire à initier un conflit majeur et ouvert. Ainsi dans le cadre d'un conflit hybride, les cibles

[6] Elie Tenenbaum, « Le piège de la guerre hybride », page 12 ;
[7] Ibid, page 15 ;

recherchées seront principalement des cibles secondaires mais adaptées au message politique recherché. En revenant à la trinité clausewitzienne de la guerre, le peuple (et ses passions), l'armée (et son intelligence), et le politique (et ses objectifs), il est possible de caractériser la guerre hybride comme une forme de guerre qui, en évitant soigneusement chacun des éléments constitutifs de cette trinité, ciblerait les relations entre chacune de ces composantes pour en perturber *in fine* la cohérence d'ensemble. Là encore, le cyberespace, support informationnel par excellence, devient un espace de confrontation majeur.

b. Un lien intime entre l'hybridité et le cyber : la cyber-hybridité.

i. Cyber-hybridité : apport du cyber à la guerre hybride.

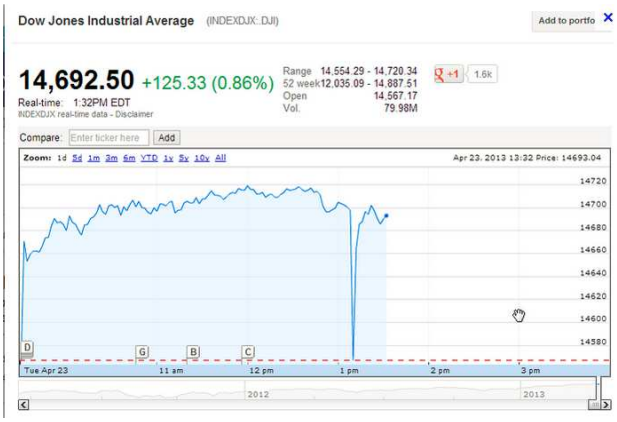
De même que la guerre hybride recouvre un champ très vaste, entre le niveau stratégique et le niveau tactique, cette cyber-hybridité peut prendre différentes formes. Tout d'abord, elle peut être vue comme l'apport du Cyber à la guerre hybride. En s'attaquant aux liens du triangle clausewitzien, elle vise à annihiler la cohérence d'ensemble de l'adversaire, avec pour objectif double de dégrader son efficacité opérationnelle tout en affectant sa volonté de combattre. A nouveau l'appui « Cyber » russe l'illustre, en visant en priorité le ressenti de la population et des forces armées tout en paralysant les échelons de commandement pour imposer *in fine* un « fait accompli ». Dans notre société interconnectée actuelle, une telle action nécessite d'agir sur l'ensemble du *Command and Control (*C2) adverse et impose de planifier puis de conduire une manœuvre « cyber-électronique ». Cette manœuvre s'inscrit dans le cadre d'une stratégie d'influence. Dans ce cadre, le Cyber est alors l'instrument du fort qui lui permet de mener des actions d'ampleur tout en limitant le risque de montée aux extrêmes.

Actuellement, la Turquie subit de nombreuses attaques informatiques[8]. Celles-ci sont revendiquées par les Anonymous en représailles à la politique actuelle turque. Néanmoins, prenant en considération l'appétence de la Russie pour les actions Cyber, et le contexte de tension diplomatique entre ces deux nations, il est permis de s'interroger sur un lien éventuel…

[8]http://www.reuters.com/article/us-turkey-internet-cybercrime-idUSKBN0U60Y820151223

ii. Cyber-hybridité : application des stratégies hybrides aux opérations Cyber.

Néanmoins, la cyber-hybridité peut également être vue comme l'application de ces principes dits hybrides à l'environnement Cyber, à savoir l'alternance d'actions conventionnelles et non-conventionnelles. Ce mode d'action permet notamment au plus faible d'exister dans le monde Cyber. En effet, il faut dès à présent battre en brèche le mythe du hacker solitaire qui, à lui seul, pourrait mettre à mal un pays. Toutes les actions Cyber significatives ont nécessité des moyens que seul un Etat est aujourd'hui en mesure de mettre en œuvre. En effet, il est très complexe pour un seul individu, voire un groupe, de disposer à la fois des moyens de renseignement amont nécessaires, et de la capacité à franchir les frontières ou « *airgap*[9] », parfois même physiques, entre les réseaux bureautiques et les réseaux métiers[10]. Le monde de l'informatique dit « métier », celui des SCADA[11], est caractérisé par son absence de normalisation, il n'existe donc pas « d'armes cybernétiques » génériques. Pour les Etats ou les organisations disposant de moyens plus limités, il n'est donc pas possible de mener des grandes opérations comme « *Olympic Games* ». Celle-ci est plus connue sous le nom de « Stuxnet », son ver informatique qui a dégradé les capacités d'enrichissement d'uranium iraniennes[12].



[9] *Airgap* : En sécurité informatique, un ***air gap*** aussi appelé ***air wall*** est une mesure de sécurité consistant à isoler physiquement un système à sécuriser de tout réseau informatique. Cette mesure, lorsqu'elle est correctement implémentée, rend toute tentative de piratage à distance impossible, quelle que soit sa sophistication.

[10] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0

[11] Supervisory Control and Data Acquisition.https://fr.wikipedia.org/wiki/Supervisory_Control_and_Data_Acquisition

[12] Là encore lire les différents ouvrages de David E. Sanger

Néanmoins, il demeure possible de mener une forme de cyber-harcèlement. « Deux explosions à la Maison Blanche, Obama blessé ». Grâce à ces quelques mots postés sur le compte tweeter de l'*Associated Press*, la *Syrian Electronic Army* (groupe de *hackers* se revendiquant proche du gouvernement syrien) a réussi à faire chuter temporairement l'indice Down-Jones de près de 130 points soit une perte temporaire de 78 milliards de dollars. (Ce qui représente l'équivalent de la dette annuelle française.) L'analyse de cette attaque met en exergue que son succès provient davantage de l'imagination des attaquants que de leur niveau technique. On imagine aisément les conséquences que pourraient avoir une succession d'attaques similaires ou, pire encore, l'absence totale de réaction de la population et/ou des marchés, saturés d'action de désinformation, face à un événement majeur.

c. Pourquoi un tel renouveau ?

Si la guerre hybride n'est pas nouvelle, c'est bien évidemment son caractère cyber combiné au nouvel équilibre entre système international et sécularisation de l'origine des pouvoirs des gouvernements qui actualise pleinement ce concept. En effet, la succession des conflits mondiaux associée à la quasi-universalité de la démocratie[13] limite aujourd'hui grandement la capacité des Etats à faire la guerre. Le général Beaufre, dans son *Introduction à la stratégie*[14], définissait déjà une forme de stratégie indirecte, *la lutte totale prolongée de faible intensité militaire* qui n'est pas sans rappeler les manœuvres russes actuelles, qualifiées de « guerre hybride ». Cette stratégie, caractérisée par le temps long, s'apparente donc à une forme de philosophie asiatique de la conflictualité, qui cherche à minimiser les affrontements directs, dont l'issue est toujours incertaine, et qui s'oppose ainsi à la vision chevaleresque occidentale qui recherche *a contrario* cet affrontement direct avec la « bataille décisive ». A ceci s'ajoute une réelle prise en compte de la notion d'influence. Le massacre et la destruction de Bagdad en 1245 par Houlagou Khan avait déjà comme objectif principal de faciliter la suite de ses conquêtes. Près de huit siècles plus tard, au plus fort des combats entre le futur *Daec'h* et les forces régulières syriennes, le *Times* titrait : « The Youtube War[15] » pour alerter sur la surenchère de vidéos postées par les deux camps, mettant en scène le sort dévolu aux

[13] Même si de nombreux états sont encore loin des standards démocratiques, ils sont aujourd'hui, à l'instar de la Chine, dans l'obligation d'assouplir leur régime.
[14] Ibid,p39 et p171
[15] http://content.time.com/time/magazine/article/0,9171,2143557,00.html

prisonniers. Si cette surenchère d'atrocités n'a, semble-t-il, pas eu de conséquences directes sur les opérations, d'autres ont en revanche eu un résultat spectaculaire.

Le cas des opérations en russe en Crimée est encore plus explicité. Bénéficiant de fait d'une connaissance très fine des infrastructures de télécommunication ukrainiennes, les forces russes ont mis en œuvre une succession d'actions de brouillage électromagnétique, de sabotage de lignes de communication et peut-être même de cyber-attaques[16], elles ont ainsi confirmé la réalité, l'actualité – mais également l'efficacité – d'une forme de « cyber-hybridité ».

Ce renouveau ne serait bien évidemment pas possible sans la numérisation globale de notre société. Celle-ci offre une opportunité majeure aux belligérants pour frapper directement la population adverse. Or l'objectif premier d'une stratégie hybride n'est-il pas d'éroder progressivement la résilience de la population adverse ?[17] Cette opportunité est d'autant plus forte au regard de la nature actuelles des différents gouvernements. Ce caractère démocratique des principaux gouvernements, source de puissance et de stabilité, apparaît comme aujourd'hui un nouveau talon d'Achille. A titre d'exemple rappelons que les terribles attentats qui ont touché Madrid en 2004 ont eu comme conséquence directe l'accélération du retrait des forces espagnoles au sein de la coalition militaire combattant en Irak au côté des Américains (même si ce retrait faisait partie du programme du nouveau premier ministre, il a néanmoins été accéléré). Au final cette cyber-hybridité permet aux Etats de s'adapter face à l'évolution du système international dans un monde figé par la dissuasion nucléaire.

d. La Cyber-hybridité renforce cette stratégie du Flou[18]

A l'opposé de la montée aux extrêmes clausewitziennes, les belligérants d'un conflit hybride sont contraints par une notion de « seuil » qui ne doit en aucun cas être franchi, au risque de sombrer dans une guerre totale conventionnelle, et donc d'avoir des conséquences négatives sans commune mesure avec les gains attendus. Pour ce faire, les belligérants vont donc utiliser tous les modes d'action possibles pour rester « sous le seuil ». Ici encore, la liste de ces modes d'action potentiels est sans fin : diplomatique, « *proxy war* [19]», déstabilisation ou mesures dans le champ économique, et bien évidemment Cyber. Depuis la fin de la guerre

[16] http://www.ceis-strat.com/fr/actu/l-emploi-des-capacites-cyber-russes-en-ukraine
[17] Elie Tenenbaum, « Le piège de la guerre hybride », page 12 ;
[18] Georges-Henri Soutou, "La stratégie du flou", *Politique Magazine*, juillet 2014;
[19] "guerre par procuration", consistant à l'emploi de "*proxy*" pour éviter toute implication directe.

froide nous vivons une évolution de plus en plus rapide du système international, ou plutôt l'application d'une forme de « Stratégie du Flou » (professeur Soutou). Dans ce contexte, le concept de guerre « hybride » repousse la séquence clausewitzienne paix-crise-guerre et évolue vers une forme « d'entropie de la conflictualité », caractérisée par sa continuité et par sa croissance en milieu « fermé ». Cette cyber-hybridité par le double anonymat qu'elle procure, à la fois par le mode d'action et à la fois par l'espace numérique, se pose aujourd'hui comme l'arme idéale dans l'environnement international actuel. Le cas de l'opération *Nitro Zeus*[20], ou du piratage de TV5 monde (même s'il n'existe aucune certitude, une action russe en représailles à la non vente des navires de type « Mistral » en serait à l'origine) illustrent ce renouveau des conflits internationaux.

II. L'emploi de la cyber-hybridité.

a. Constat sur l'emploi des capacités cyber

i. Le cas russe :

La Russie est certainement la nation qui a intégré un appui Cyber au plus près de ses opérations militaires, notamment en Géorgie en 2008, puis en Crimée en 2014. Néanmoins, il ressort que ces deux conflits se caractérisent par leur aspect hybride. Il est également intéressant de noter que les capacités cyber initialement utilisées au niveau stratégique (visant principalement les grandes infrastructures numériques par des actions de types DDos[21])[22] sont aujourd'hui mise en œuvre à un niveau opératif. Les opérations menées par la suite en Crimée avaient clairement des objectifs beaucoup plus ambitieux, visant l'intégralité du lien télécom de la péninsule[23]. Les informations sont encore peu nombreuses sur la réalité des actions menées, mais les quelques disponibles nous permettent d'imaginer qu'un plan de manœuvre a été exécuté mettant en œuvre des actions d'ensemble (brouillage) et des actions ciblées (action sur les téléphones de dirigeants, coupure de câble) avant de faire l'objet d'une phase d'exploitation au travers d'une stratégie militaire/nationale d'influence. De façon beaucoup

[20] Opération Numérique d'ampleur visant la République Islamique d'Iran en cas d'échec des négociations sur le nucléaire Iranien.
[21] *Deny Of Service,* ou *Distributed Deny Of Service* est une attaque informatique visant à saturer le serveur ciblé pour le rendre inutilisable, *a minima* le temps de l'attaque, voire jusqu'à une intervention de maintenance.
[22] CEIS, *Observatoire du monde Cybernétique,* DAS, Mars 2014, 25p, page 15.
[23] Julien Lepot, http://www.ceis-strat.com/fr/actu/l-emploi-des-capacites-cyber-russes-en-ukraine

plus fine, les planificateurs russes ont ainsi su exploiter la couverture médiatique de leur intervention en Crimée. Bénéficiant du relais des grandes agences médiatique russes, ils ont su générer ce sentiment de débordement malgré un rapport de force localement défavorable à la Russie : 10 000 Russes (principalement des *Spetnatz* ou des commandos aéroportés) contre 16 000 Ukrainiens[24]. Nul doute que la succession de reportages montrant la reddition de casernes loyalistes a généré ce sentiment, tout en créant un effet « boule de neige ». C'est donc bien la combinaison entre une manœuvre d'influence et l'isolement « informationnel » de la Crimée, en privant ainsi les forces ukrainiennes en présence de directives de Kiev qui a permis cette action. Pour réaliser cette manœuvre d'isolement, nul doute que les forces russes se sont appuyées sur une connaissance très fine des infrastructures de télécommunication ukrainiennes, probablement installées et soutenues par des entreprises russes…

Pour renforcer le caractère hybride de ces actions, il est intéressant de noter que pour bon nombre, ces actions ont été menée par des tiers. Ainsi l'étude des actions menées contre la Géorgie en 2008 permet de remonter à un réseau de cyber Criminel « *Russian Business Network* »[25]. L'emploi d'un tiers en appui d'une action directe des forces armées russes peut paraitre surprenant en premier abord. L'objectif d'une telle manœuvre est certainement d'augmenter davantage le flou tant sur l'origine de l'attaque que sur la réalité des capacités cyber russes.

ii. Le cas de la Chine :

Alors que la Chine a été un des pionniers à recoloniser sous le prisme Cyber le concept de guerre hybride, « la guerre hors limite [26]» ; elle est aujourd'hui très discrète sur ce sujet[27]. Même si ne fait guère de doute qu'elle use fortement du cyber-espionnage, elle n'a pas démontré à ce jour une volonté de mettre en œuvre de capacités offensives, ni même de les intégrer dans des opérations militaires. Néanmoins, il convient de rester particulièrement prudent car ce type de capacité est intiment lié à la préservation du secret.

Concernant le cyber-espionnage, de nombreuses études visant à en évaluer l'ampleur ont été menées. Celles-ci ne seront pas évoquées dans le présent document, car d'une part

[24] Janis Berzins, *Russia's new generation warfaire in Ukraine: Implications for Latvian Defence Policy*, National Defence Academy of Latvia, 2014, 13p.
[25] CEIS, *Observatoire du monde Cybernétique,* DAS, Mars 2014, 25p, page 13.
[26] Liang Qiao, Xiangsui Wang, *La Guerre hors limites*, RIVAGE, 309p, 2006.
[27] http://www.iris-france.org/62048-les-defis-que-pose-tranquillement-la-chine-a-loccident/

elles sont sujettes à caution et que d'autre part elles n'apportent que peu d'intérêt à cette étude. En revanche, le silence de la Chine pourtant pionnière (à la fois sur le concept de guerre hybride et à la fois dans le domaine du Cyber), et qui est probablement l'unique pays à maîtriser pleinement son Internet, est particulièrement surprenant dans son objectif actuel de s'imposer comme un concurrent des Etats-Unis.

iii. Le cas US :

L'emploi des capacités cyber américaine pourrait se résumer de la façon suivante : « faire autrement ». Encore une fois, s'il n'est pas possible de parler directement de guerre hybride, une certaine analogie reste envisageable. Dans le cadre d'une guerre totalele Cyber vise en premier lieu le C2 adverse. L'interconnexion des moyens de communication est tel qu'il est aujourd'hui inenvisageable de dissocier les systèmes d'informations des systèmes de communication. La dernière version du *Field-Manuel 3-38,* manuel de référence pour les opérations terrestres US, précise la nécessité d'inclure, à un niveau tactique, la prise en compte de ce double domaine de l'appui cyber-électronique. Il est alors nécessaire d'étendre ce concept à la cyber-hybridité. En effet, tous les exemples précédents n'ont de sens que par une approche qui englobe, outre l'information en elle-même (liée à la stratégie d'influence), son support et son système d'information.

L'emploi des capacités cyber US se résume d'une part à la recherche et la neutralisation de cibles à haute valeur ajoutée[28]. On imagine facilement les conséquences de ces actions, comme l'envoi d'un SMS invitant la cible à un rendez-vous afin de l'appréhender (ou de le neutraliser par un tir de drone armé), en termes de résilience du groupe armé. Cette forme plus conventionnelle au niveau opératif nous amène vers un concept « d'opérations cyber-spéciales ». A l'instar de celles-ci, l'utilisation des capacités cyber est orientée avant tout à des fins de renseignement puis de déception voire de neutralisation pour des individus à haute valeur ajoutée.

Au niveau stratégique, l'emploi des capacités cyber US se rapproche plus fortement du concept de guerre hybride. Il s'agit de viser directement la confiance d'une population envers son dirigeant. Son emploi sous une forme non-conventionnelle comme ce fut le cas lors de

[28] Shane Harris, *@WAR : The rise of the Military-Internet Complex*, Eamon Dolan/Houghton Mifflin Harcourt, 2014, 263p.

l'opération "*Olympic Game"* et plus récemment avec la probable opération "*Nitro Zeus"* nous rappelle combien l'emploi de l'arme cyber est adapté aux relations internationales modernes.

iv. Constat sur l'usage du cyber-espace par les groupes terroristes et/ou de la cyber-criminalité.

L'intérêt des groupuscules djihadistes pour l'environnement numérique est très marqué. Les attentats du 11 septembre avaient déjà mis en lumière l'utilisation du cyberespace, que ce soit pour le recrutement, la coordination ou même la formation. Néanmoins, concernant le groupe *Daec'h* il existe un véritable paradoxe. Il a envahi massivement le cyberespace, notamment au travers de ses réseaux de recrutement, de ses productions vidéo ou de son magazine de propagande numérique *Dabiq*. Véritable clé de voûte de son organisation, le recrutement des combattants étrangers se fait largement par le biais du cyberespace. Il est, à cet égard, intéressant de s'interroger sur l'absence d'action d'envergure sur ce terrain de confrontation. Outre le fait, déjà évoqué, de la nécessité de disposer d'une organisation conséquente pour mener des cyberattaques, une autre explication peut venir du rejet de la communauté « *underground* ». En effet, à l'instar des Anonymous, de nombreuses « #Op »[29] ont été lancées contre le groupe, alors même que celles lancées par les sympathisants du groupe n'ont jamais réellement abouti[30]. Néanmoins la seule action qui pourrait lui être rattachée (même si cela reste fortement sujet à discussion) est le possible piratage de TV5 Monde. Celui-ci doit en outre être relativisé car très probablement, contractualisé auprès d'un tiers[31]. Ceci prouve qu'une partie de la menace est du ressort de la cybercriminalité. Cette « criminalité » est aujourd'hui un acteur incontournable de l'hybridité. Elle permet aux Etats d'agir avec un anonymat renforcé, donc avec un niveau de bruit faible et un risque de montée aux extrêmes limité.

---

[29] #OP est le terme utilisé pour identifier les opérations menées par les Anonymous sur internet. http://www.telegraph.co.uk/news/worldnews/islamic-state/12003242/OpISIS-Why-Anonymous-has-declared-an-online-war-against-Isil-in-90-seconds.html

[30] http://www.zataz.com/des-pirates-de-daech-sattaqueraient-de-nouveau-a-la-france/ http://echoradar.eu/2015/02/11/opfrance-la-bataille-de-la-desinformation-et-lavenement-du-cybervandalisme/

[31] De nombreuses thèses ont été émises par rapport à cette attaque. Certains considèrent que cette attaque pourrait être une représailles russe suite au refus français de livrer les BPC Mistral. http://www.france24.com/fr/20150610-piratage-cyberattaque-tv5-monde-russes-hackers-piste-enquete-ei-jihadistes

b. Les enseignements.

i. Le Cyberespace un carrefour entre l'environnement technique et l'espace cognitif :

Il ressort des lignes précédentes quelques enseignements majeurs. En premier lieu, l'emploi des capacités cyber ne peut être dissocié de l'emploi des capacités de guerre électronique, comme le prouvent les récentes études exploitant les ondes radars comme « point d'entrée » vers le réseau ciblé[32]. Ce combat « cyber-électronique » jouera sans nul doute un rôle de plus en plus prépondérant dans les opérations militaires futures, principalement celles menées à l'encontre d'une force plus conventionnelle[33].

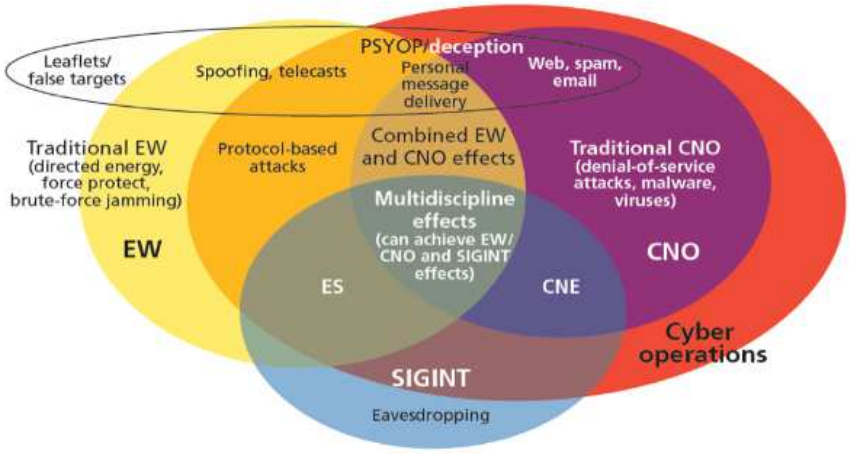


Figure 1. Functional View of Converging Areas According to CERDEC Draft (Reprinted from Porche, et al., "Redefining Information Warfare Boundaries for an Army in a Wireless World," p.51)

En outre, comme l'ont illustrés les opérations russes en Crimée, l'utilisation de cette hybridité « cyber-électronique » doit s'inscrire dans une stratégie nationale d'influence qui va au-delà d'une simple stratégie militaire d'influence. Sans forcément franchir la frontière des « *black PSYOPS* », la reprise par la grande majorité des médias d'une analyse favorable à l'état final recherché sera d'autant plus efficace qu'une forme de « suprématie informationnelle » aura été établie. Bien souvent le cyber n'est dans ce cadre qu'un vecteur concourant à l'acquisition de cette suprématie.

[32] http://www.cyberdefensereview.org/2016/01/04/convergence-of-cyberspace-operations-and-electronic-warfare-effects/

[33] Aymeric Bonnemaison, Stéphane Dosse, *Attention Cyber ! : vers le combat cyberélectronique,* Economica, 2014, 224p.

Dans tous les cas, ces actions « cyber-hybride » nécessitent une planification particulièrement rigoureuse. D'une part, car l'on imagine facilement l'important effort renseignement préalablement nécessaire ; d'autres part que des probables phases de "*shaping"* sont nécessaires pour acquérir une garantie de réussite. En outre, ces actions sont d'autant plus efficaces qu'elles s'inscrivent dans une manœuvre interarmées plus large. Là encore les exemples russes et surtout américains en Irak sont exemplaires.

ii. Cyber-hybridité contre Cyber-dissuasion ?

Durant le début des années 2000, de nombreux penseurs envisageaient que le Cyber pourrait être l'instrument d'une nouvelle forme de dissuasion amenée à suppléer, *a minima*, la dissuasion nucléaire. Pourtant, faute d'un « Hiroshima numérique » préalable, cette forme de dissuasion ne s'est jamais instaurée. Néanmoins, sous la forme de « Cyber-hybridité », une nouvelle forme de « riposte graduée », proche de la théorie de « l'ultime avertissement » peut exister. Il n'y a donc pas lieu d'opposer dissuasion et cyber. Au contraire, ils sont maintenant complémentaires. Si la première permet de figer le système international en limitant au maximum l'apparition d'un nouveau conflit majeur, le second, notamment sous sa forme hybride, permet une forme de dialectique de la conflictualité dans ce système figé.

iii. La non-létalité de l'arme cyber, un principe ?

Peu de nations, comme la France, affichent une doctrine cyber claire. Pour sa part la France a annoncé qu'elle ne frapperait pas en dehors d'un conflit. On peut donc s'interroger si la France ne refuserait pas cette forme de cyber-hybridité ? Au contraire, il devient de plus en plus évident que cette zone de liberté pour les Etats ne pourra perdurer si la frontière de la létalité venait à être franchie. Dans ce cas, les Etats, devant être en mesure de garantir à sa population un niveau acceptable de sécurité, ne pourront plus tolérer l'existence d'une telle menace. Il s'en traduira une augmentation drastique du contrôle étatique sur le cyberespace à l'instar de ce que l'on peut entrevoir dans certains Etats moins démocratiques… Au niveau mondial, il y aura donc un choix entre l'alternative à la dissuasion nucléaire, sous forme d'ultime avertissement, que nous avons précédemment évoqué et la poursuite de cette « cyber-hybridité ».

iv. Un droit international dépassé ?

Alors que les premières grandes actions Cyber, majoritairement sous une forme hybrides, ont déjà eu lieu sous diverses formes (*Snake Uroburos, Flame,…*) aucune action judiciaire internationale n'a jamais débouché. En parallèle, la gouvernance d'internet et en particulier le contrôle de l'ICANN fait toujours l'objet d'un débat acharné entre les grands de l'Internet. Dans les faits, ce contrôle reste globalement à la main des Américains. La récente déclaration du président Obama, le 18 février 2015, ne fait que confirmer cette réalité : « Nous avons possédé Internet. Nos entreprises l'ont créée, l'ont développée et l'ont améliorée de telle manière que l'Europe ne peut pas lutter ». Si cette déclaration s'adressait à ses alliés européens, on imagine facilement la réalité de la position US vis-à-vis de la Chine ou de la Russie… C'est en particulier avec cette dernière que la bataille pour la gouvernance de l'internet est la plus forte.[34]

L'absence de preuves formelles, qu'offre l'action dans le cyberespace, n'est pas compatible avec une forme de « justice internationale ». Même si une ultime conviction existe, elle ne semble pas être juridiquement suffisamment forte, tout du moins lorsque le risque demeurera acceptable par les grandes nations, pour être prise en compte par la communauté internationale. A nouveau, cette cyber-hybridité restera donc la norme, tant que la frontière de la létalité ne sera pas franchie, générant alors un probable changement de paradigme.

[34] http://ultimaratio-blog.org/fr/archives/5737

Conclusions :

Le terme de « Guerre Hybride » est aujourd'hui discutable car il regroupe aujourd'hui des concepts très différents. Les exemples russes mais également l'action de Daech sur le théâtre irako-syrien illustrent l'ampleur de cette nouvelle forme de conflictualité. Néanmoins, ces concepts correspondent à une évolution de la conflictualité qui viserait une forme d'érosion de l'adversaire en évitant au maximum « la bataille décisive ». Pour aboutir à cette érosion, deux cibles peuvent être privilégiées, le système de commandement adverse (le *Command and Control ou* C2) et la population civile ; cette seconde étant aujourd'hui la source du pouvoir des grandes nations.

Quelle que soit la cible envisagée, elle est aujourd'hui vulnérable d'un point de vue cyber tant notre société est aujourd'hui numérisée et donc dépendante du cyberespace. Ainsi cette notion d'hybridité est intimement liée à la notion de cyber, donnant naissance à un phénomène de cyber-hybridité. Ce phénomène peut être vu selon deux prismes différents : d'une part l'apport du domaine cyber à cette nouvelle forme de conflictualité, et d'autre part l'application de ces principes « hybrides » au domaine cyber. Outre, la relation entre la cible et le moyen, le Cyber, est aujourd'hui un facteur clé de la résurgence de cette nouvelle forme de conflictualité. En effet, dans le système international actuel, figé globalement par la dissuasion nucléaire, il offre aux différents Etats de maintenir une forme de conflictualité, comme autant de frappes préventives. Les récentes révélations sur l'opération "*Nitro Zeus*" tendent à le démontrer à nouveau. Alors que la doctrine nucléaire est généralement celle de « la non-utilisation en premier (*No first use)* », l'utilisation des capacités Cyber s'apparente aujourd'hui à une forme « d'ultime avertissement ». En outre, l'emploi des capacités Cyber offre une forme d'anonymat. Même s'il est toujours possible d'arriver à une « forme de conviction » de l'origine de l'attaque, le flou résiduel offre la capacité de poursuivre aisément les négociations au niveau diplomatique.

Les dernières années ont mis à mal le mythe du hacker solitaire. Au mieux, un groupe de hackers peut exécuter une forme de cyber-harcèlement par une succession de petites attaques. Au contraire, les seules opérations d'ampleur ont mis en exergue leur complexité et la largeur du champ d'action nécessaire à de telles opérations. Ainsi pour exister dans le cyber-espace, les plus petits Etats ou organisations doivent faire en sorte d'agir en permanence. C'est donc dans ce cadre, en particulier pour les organisations terroristes, que l'application des principes

hybrides au monde Cyber revêt un intérêt certain. Leur objectif étant de viser la résilience de la population, il leur est donc nécessaire de privilégier une permanence des actions pour servir de caisse de résonnance à une unique action d'ampleur.

Dans le cadre des opérations militaires, cette cyber-hybridité s'inscrit dans le cadre d'une stratégie militaire d'influence et ne peut être traitée indépendamment des capacités de guerre électronique car une grande partie de leur périmètre respectif est commun. Ce double aspect dual nécessite une prise en compte bien spécifique par le chef militaire. En effet, cette stratégie militaire d'influence doit s'inscrire dans le cadre plus large d'une stratégie gouvernementale d'influence, au risque de produire des effets contre-productifs.

Cette dématérialisation du conflit, offre l'opportunité aux Etats, d'employer des belligérants privés pour augmenter le flou. Au regard des importants investissements dans la cyberdéfense, il est probable que le cyberespace devienne de plus en plus un espace de conflit selon l'adage de M. de Talleyrand[35]. Il est alors permis de s'interroger si l'apparition dans le concert des nations d'intervenants privés capables de mener un « *Pearl Harbor* numérique [36]» ne remettrait pas en question la primauté des Etats sur la scène internationale. Pourtant il demeure essentiel que le pas de la létalité directe de l'action Cyber ne soit pas franchi, au risque de mettre à mal cette capacité de frappes préventives et d'ultime avertissement qu'elle offre aujourd'hui.

[35] « On peut tout faire avec des baïonnettes sauf s'assoir dessus. »
[36] Discours de Léon Paneta, secrétaire de la défense américain, peu de temps après l'attaque contre l'Aramco

Elément de Bibliographie:

Ouvrages:

- Shane Harris, *@WAR : The rise of the Military-Internet Complex*, Eamon Dolan/Houghton Mifflin Harcourt, 2014, 263p.
- Aymeric Bonnemaison, Stephane Dosse, *Attention Cyber ! : vers le combat cyberélectronique*, Economica, 2014, 224p.
- Général André BEAUFRE, *Introduction à la stratégie*, Pluriel, 2012 (1963), 192p.
- Karl von Clausewitz, *De la guerre, Ellipses, 2014(1832), 154p.*
- Liang Qiao, Xiangsui Wang, *La Guerre hors limites*, Rivage, 2006, 309p.

Articles de presses :

- David E. Sanger, *New-York Times*, Nombreux articles.
- http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0

Etudes :

- Georges-Henri Soutou, *La stratégie du flou*, *Politique Magazine*, juillet 2014.
- Janis Berzins, *Russia's new generation warfaire in Ukraine : Implications for Latvian Defence Policy*, National Defence Academy of Latvia, 2014, 13p.
- Elie Tenenbaum, *Le piège de la guerre hybride*,IFRI, 2015, 51p.
- CEIS, *Observatoire du monde Cybernétique*, DAS, Mars 2014, 25p.
- *Field Manual 3.38 Cyber-Electronic Activities*, US ARMY, 2014, 96p.
- Dr. Phillip A. Karber, *« Lessons Learned » from the Russo-Ukrainian War*, The Potomac Fundation, 2015, 50p.
- LCL Hyacinthe de Lavaissière, *La nouvelle arme Cyber se construit au sein de l'US Army*, Cahier du CESAT, 2015, 3p

Autres sites internet :

- http://www.ceis-strat.com/fr/actu/l-emploi-des-capacites-cyber-russes-en-ukraine
- http://content.time.com/time/magazine/article/0,9171,2143557,00.html
- http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx
- http://www.reuters.com/article/us-turkey-internet-cybercrime-idUSKBN0U60Y820151223
- http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0
- http://www.cyberdefensereview.org/2016/01/04/convergence-of-cyberspace-operations-and-electronic-warfare-effects/
- http://www.lemonde.fr/international/article/2014/10/06/le-fbi-accuse-la-chine-de-cyberespionnage_4500894_3210.html