Les penseurs de la stratégie sous le prisme contemporain

Fabio RIGAUD
Chercheur - Pôle Armées
Institut d'Études de Géopolitique Appliquée

Septembre 2021

ISSN : 2739-3283

Comment citer cette publication :

Fabio Rigaud, « Les penseurs de la stratégie sous le prisme contemporain » Institut d'Études de Géopolitique Appliquée, Paris, 27 septembre 2021.

Institut d'Études de Géopolitique Appliquée - 31 Rue de Poissy 75005 Paris
E-mail : secretariat@institut-ega.org
Site internet : www.institut-ega.org

SOMMAIRE

Introduction – P. 2

Les penseurs de la stratégie face à l'évolution des terrains d'affrontement – P. 3

La guerre dans le domaine spatial : de nouvelles considérations stratégiques ? – P. 3
Le cyberespace comme cinquième milieu stratégique : vers une guerre à distance – P. 6

L'analyse des conflits armés sous la perspective des penseurs de la guerre – P. 10

Mutations des enjeux doctrinaux et des conditions de victoire – P. 10
Vers un retour à la guerre de haute intensité et une résurgence des penseurs classiques ? – P. 14

Le caractère de la Guerre évolue en dépit de la récurrence des conflits armés. Malgré le retour de l'ombre d'une guerre dite « de haute intensité », nous assistons depuis une vingtaine d'années à davantage de conflits asymétriques, de guerres civiles, ou de conflits hybrides. L'arrivée d'Internet et la transmission rapide de l'information à travers le monde ont également contribué à transformer les méthodes de guerres en créant de nouvelles vulnérabilités et donc de cibles potentielles. De même, les nouvelles technologies de l'information et de la communication ont rendu l'opinion publique davantage perméable aux influences extérieures et peuvent servir à propager des idées, légitimer ou non un conflit en interne et à l'international, ou encore renforcer l'opposition dans un État ennemi. Le cyberespace est donc devenu un nouveau terrain de confrontation militaire, enchâssé dans les terrains d'affrontements classiques.

La pensée stratégique s'est développée au gré des évolutions technologiques : si l'on tente de schématiser succinctement l'évolution de la pensée stratégique, celle-ci s'est d'abord intéressée aux armées régulières, avec Sun Tzu ou Clausewitz, puis a évolué pour inclure la guerre maritime, aérienne, blindée, la dissuasion nucléaire et, désormais, la cyberguerre. Pour autant, des thèmes communs comme la sélection des objectifs stratégiques peuvent être identifiés. Des analyses et concepts ont gardé leur valeur à travers le temps malgré l'évolution des techniques.

Ainsi, face aux évolutions de la forme et des méthodes de guerre, les grands penseurs de la stratégie peuvent-ils encore offrir des clefs de lecture pour l'analyse et la compréhension des conflits armés ?

I. Les penseurs de la stratégie face à l'évolution des terrains d'affrontement

La Guerre a connu des évolutions majeures depuis les auteurs classiques. De nouveaux terrains d'affrontement sont apparus et, avec eux, de nouvelles méthodes de faire la guerre. Les auteurs classiques ont-ils gardé leur pertinence dans l'analyse des conflits dans les nouveaux milieux stratégiques que sont l'espace extra-atmosphérique et le cyberespace ?

La guerre dans le domaine spatial : de nouvelles considérations stratégiques ?

La pensée stratégique a évolué au gré des terrains d'affrontements, créant plusieurs écoles de stratégie classiques. La plus ancienne est l'école terrestre, représentée par des penseurs tels que Sun Tzu, Carl Von Clausewitz ou le baron de Jomini. Avec la maitrise de la navigation, de nouveaux auteurs ont théorisé la guerre maritime, les plus connus étant Alfred Mahan et Julian Corbett. Enfin, de manière similaire, l'apparition de l'aviation a rendu nécessaire la théorisation de la pensée stratégique appliquée à travers Giulio Douhet. Aujourd'hui, le développement de nouveaux terrains d'affrontement - nommément, le milieu cyber et l'espace extra-atmosphérique - crée de nouvelles questions en termes de stratégie.

Le domaine spatial pourrait répondre à des problématiques similaires à l'espace aérien : il s'agit d'un espace sans obstacle, dit fluide, qui permet de naviguer autant au-dessus de la terre que de la mer.

En 2020, cette similarité et la connexion géographique entre les deux milieux ont notamment poussé la France à renommer son Armée de l'Air en *Armée de l'Air et de l'Espace*.

Des différences majeures entre les deux milieux stratégiques peuvent cependant être mises en exergue : d'abord, le domaine spatial n'a pas de frontière et n'appartient à personne, il est donc possible de survoler un autre État sans son autorisation, facilitant les activités d'espionnage. Ensuite, les moyens offensifs attribués au domaine spatial sont plus limités. En particulier, contrairement au domaine aérien, le déploiement d'armes de destruction massive dans l'espace est prohibé[1]. Les satellites, à la différence des avions, ont une trajectoire prédéfinie et prévisible : une orbite. Ainsi, si la capacité de l'aviation à se mouvoir librement dans l'espace en faisait, selon Douhet, « l'arme offensive par excellence »[2], les satellites sont davantage des cibles stratégiques que des moyens d'offensive militaire, justifiant la priorité donnée au développement de moyens de défense.

Everett Dolman divise l'espace en quatre zones auxquelles répondent des considérations stratégiques spécifiques[3] :

- la zone *Terra*, qui s'étend de la surface terrestre jusqu'à la frontière de l'espace, soit la ligne de Karman, où l'atmosphère n'est plus suffisamment dense pour permettre à un avion de voler,
- la zone *Terran*, soit l'espace circumterrestre, qui s'étend de l'orbite exploitable la plus basse jusqu'après l'orbite géostationnaire,
- la zone *Lunar*, de l'orbite géostationnaire jusqu'après l'orbite lunaire. La lune pourrait notamment représenter une base pour des projections à plus longue distance ou être exploitée pour ses ressources,
- la zone *Solar,* au-delà de l'orbite lunaire jusqu'aux confins du système solaire.

Au sein de l'espace circumterrestre, les différentes orbites revêtent des caractéristiques particulières. L'orbite géostationnaire est la plus disputée : pour être capables de rester immobiles par rapport à un point

[1] Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, ouverte à la signature le 27 janvier 1967, entrée en vigueur le 10 octobre 1967, *RTNU,* vol.610, p.222.
[2] DOUHET Giulio, *The Command of the Air*, Maxwell, Air University Press, 2019, p.14.
[3] DOLMAN Everett, *Astropolitik. Classical Geopolitics in the Space Age,* Londres, Routledge, 2005, p.60.

terrestre donné, les satellites suivent une orbite unique, concentrique à l'équateur. Ainsi, le nombre de satellites en orbite géostationnaire est nécessairement limité, en faisant un espace de compétition privilégié.

La deuxième orbite clef est l'orbite de basse altitude. Les satellites en orbite basse ont l'avantage d'offrir des transferts de données plus rapides avec la surface terrestre. Leur proximité permet également l'obtention d'images de meilleure résolution que des satellites disposés sur des orbites plus hautes, leur conférant un rôle central dans les activités de reconnaissance et d'espionnage.

En transposant la théorie de Halford Mackinder sur le *Heartland* au domaine spatial, Everett Dolman affirme que « celui qui contrôle l'orbite terrestre basse contrôle l'espace circumterrestre proche. Celui qui contrôle l'espace circumterrestre proche domine Terra. Celui qui domine Terra détermine le destin de l'humanité. »[4]

Dolman identifie des points clefs qui garantissent la domination de l'espace circumterrestre. Ainsi, il fait l'analogie entre les routes maritimes, dont le contrôle a permis la domination britannique sur les mers selon Mahan et les orbites de transfert d'Hohmann, lesquelles permettent de changer d'orbite de la manière la plus efficace possible[5].

Dans une doctrine conjointe sur les opérations spatiales, les États-Unis confirmaient de manière explicite leur volonté d'obtenir un contrôle de l'espace à travers des moyens offensifs comme défensifs dans le but d'assurer la liberté d'action des États-Unis et de leurs alliés tout en niant, s'ils le souhaitent, cette dernière à leurs adversaires[6] .

[4] *Ibid,* pp.6-7.
[5] *Ibid,* p.64.
[6] Joint Chiefs of Staff, *Space Operations,* Joint Publication 3-14, 10 avril 2018, incorporant les changements du 26 octobre 2020, I-4.

Plusieurs États ont déjà produit des missiles capables de détruire des satellites en orbite basse; en l'occurrence les États-Unis, la Russie, la Chine et l'Inde[7]. En 2019, la ministre des Armées françaises Françoise Parly a exposé une stratégie spatiale de défense pour la France. Cette stratégie inclut également une forme de militarisation de l'espace circumterrestre à but défensif avec le développement, présenté en 2020, de patrouilleurs spatiaux « YODA » chargés de protéger les satellites français[8].

Le cyberespace comme cinquième milieu stratégique : vers une guerre à distance

En parallèle des quatre terrains d'affrontements que sont la terre, la mer, l'air et l'espace, le milieu stratégique cyber crée un défi important pour la pensée stratégique classique, qui considère la guerre comme un affrontement physique. Pourtant, la pensée stratégique des auteurs classiques, en dehors de ses éléments les plus dépendants à la notion de territoire, peut trouver de l'intérêt dans le domaine immatériel.

Selon Sun Tzu, le sommet du talent n'était pas d'obtenir des victoires en donnant bataille, mais plutôt de « subjuguer l'ennemi sans combattre »[9]. En ce sens, le cyberespace représente un milieu stratégique idéal en ce qu'il permet d'infliger des dommages à l'adversaire sans confrontation physique et, possiblement, de manière anonyme. En termes tactiques également, la cyberguerre revêt un avantage non négligeable : du fait de la numérisation croissante de l'ensemble des secteurs de la société, le cyberespace est devenu un milieu stratégique transversal, qui affecte les autres terrains d'affrontement.

[7] « L'Inde annonce avoir détruit un satellite en orbite avec un missile », *Le Monde*, 27 mars 2019.
[8] Avis n°3465 Tome VI, Défense. Préparation et emploi des forces : Air, 21 octobre 2020, *Commission de la Défense Nationale et des forces armées*, p.58.
[9] SUN Tzu, *The Art of War*, Londres, Oxford University Press, 1963, p.77.

Le cyberespace est traditionnellement divisé en trois couches[10] : la première est la couche physique, qui comporte les appareils terminaux (téléphones, ordinateurs…) et les infrastructures matérielles qui permettent le transfert de l'information (câbles, serveurs…). Cette première couche représente une cible d'action directe à des fins d'offensive ou d'espionnage : les câbles sous-marins peuvent par exemple être coupés en temps de guerre ou les États peuvent se brancher dessus pour intercepter les données y transitant. La deuxième couche est la couche logicielle, composée de programmes qui permettent l'interaction homme-machine et la transmission de l'information entre machines au sein d'un réseau. Cette couche intermédiaire comporte davantage de vulnérabilités et offre des opportunités aux attaquants tant en termes d'espionnage que de capacité offensive, à travers des attaques par déni de service, des programmes malveillants, virus, logiciels espions, etc. La dernière couche est la couche cognitive, formée des informations ou contenus échangés à travers Internet. Ainsi, des attaques sur cette couche visent à influencer la perception des individus à travers des opérations de désinformation ou de propagande, par exemple avec l'utilisation de bots.

Pour Thomas Rid, les cyberattaques motivées politiquement ne sont que « des versions sophistiquées de trois activités aussi vieilles que la guerre elle-même : le sabotage, l'espionnage et la subversion. »[11] Ainsi, aux trois couches correspondent des cyberattaques spécifiques : les deux premières constituent des cibles potentielles pour l'espionnage ou le sabotage ; la troisième peut être utilisée à des fins de subversion. L'importance des flux d'information qui transitent à travers le cyberespace en fait le milieu stratégique clef de l'espionnage moderne. Les penseurs de la stratégie classique avaient déjà mis en évidence l'importance de l'information comme facteur de la guerre. Sun Tzu affirmait ainsi « connais l'ennemi et connais-toi toi-même ; sur cent

[10] « Rapport d'Information sur la cyberdéfense », *Commission de la Défense Nationale et des Forces Armées*, 04 juillet 2018.
[11] RID Thomas, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 2012, Vol.35 (1), p.6.

batailles tu ne seras jamais en péril. »[12] De la même manière, selon Clausewitz, le manque de fiabilité de l'information est tel un brouillard qui s'étend sur la guerre et rend la contingence impossible à maîtriser. En ce sens, le cyberespace étant devenu le domaine clef du transit d'informations, il représente un champ de bataille parallèle pour réduire l'incertitude tout en augmentant celle de l'adversaire. Ainsi, les cyberattaques peuvent être utilisées afin d'épaissir le brouillard du côté de l'adversaire en détruisant ou altérant les informations à sa disposition.

En dehors de l'espionnage, le cyberespace et plus particulièrement sa couche logicielle, est le lieu de la cyberguerre. Richard Clarke et Robert Knake définissent cette dernière comme « les actions d'un État-nation visant à pénétrer les ordinateurs ou réseaux d'une autre nation dans le but de causer des dommages ou des perturbations. »[13]

À moyens égaux, la guerre dans le cyberespace avantage l'offensive. L'attaquant a le choix des cibles ; il peut donc investir autant de moyens qu'il le souhaite dans son attaque. Le défenseur, en revanche, est contraint de diviser ses moyens entre les cibles qu'il souhaite protéger. De même, pour une cible précise, une seule vulnérabilité est suffisante pour ouvrir l'accès à l'ordinateur ciblé. Le défenseur, en revanche, doit identifier toutes les vulnérabilités potentielles pour être complètement protégé[14]. Le milieu cyber est cependant plus propice à l'automatisation. Par conséquent, la boucle OODA (Observer – Orienter – Décider-Agir) chère à Boyd s'effectuerait le plus rapidement possible à la vitesse de l'algorithme dans ce milieu. Ainsi, l'avantage de l'offensive peut être relativisé par la supériorité du codage de l'outil.

[12] *Ibid.*, p.84.
[13] CLARKE Richard A., KNAKE Robert K., *Cyber War : The Next Threat to National Security and What to Do About It*, New York, HarperCollins e-books, 2010, p.11.
[14] KREPINEVICH Andrew F., *Cyber Warfare. A "Nuclear Option" ?*, Center for Strategic and Budgetary Assessment, Washington, 2012, p.40.

Antoine Henri de Jomini, en parlant du conflit terrestre, affirmait comme l'un des principes fondamentaux de la guerre le fait de « jeter la masse des forces sur le point décisif »[15]. Transposé à la cyberguerre, le cœur de la stratégie devient l'identification de ces points décisifs, lesquels sont « ceux capables d'exercer une influence marquée sur le résultat de la campagne ou sur une entreprise unique »[16]. Ces points représentent des fragilités, des centres névralgiques dont la destruction ou l'altération paralysent les institutions ou impactent de manière considérable le fonctionnement du pays attaqué.

Comme mis en avant par Douhet au sujet de l'aviation, le champ de bataille de la cyberguerre n'a pour limites que les frontières des États en guerre, supprimant la distinction entre soldats et populations. Ainsi, plusieurs attaques par déni de service distribués (DDoS) ont pu avoir lieu ; par exemple, contre les sites d'institutions gouvernementales et de banques en Estonie en 2007[17] ou à plusieurs reprises contre le réseau électrique ukrainien[18]. Pourtant, malgré leur potentiel catastrophique, les opérations de cybersabotages ont gardé un aspect limité, bien que fortement incapacitant, voire neutralisant. Bertrand Boyer indiquait que « le combat numérique permet […] de conduire une forme de guérilla quotidienne qui ne cherche pas à détruire son adversaire, mais dans laquelle les défenseurs s'épuisent à tenter de parer chaque coup. »[19] Ce dernier précise que de telles méthodes de combats sont utilisées non seulement par des acteurs infra-étatiques mais également par des États cherchant à infliger des dommages de manière indirecte.

Selon Clausewitz, la destruction de l'ennemi demeure en effet un simple moyen au service d'une fin politique. Ainsi, trois éléments

[15] JOMINI Antoine Henri, *The Art of War*, Kingston, Legacy Books Press, 2008, p.48.
[16] *Ibid*, p.60.
[17] HERZOG Stephen, « Revisiting the Estonian Cyber Attacks : Digital Threats and Multinational Responses », *Journal of Strategic Security*, 2011, Vol. 4(2), p.51.
[18] JEWKES S., POLITYUK P., VUKMANOVIC O., « Ukraine Power Outage was a Cyber-Attack : Ukrenergo », *Reuters*, 18 janvier 2017.
[19] BOYER Bertrand, *Guérilla 2.0. Guerres irrégulières dans le* cyberespace¸ Paris, Editions de l'Ecole de Guerre, 2020, p.24.

peuvent être conquis pour emporter la victoire : « Les forces armées, le territoire et la volonté de l'ennemi »[20]. En ce sens, la guerre est une épreuve de force[21] : une simple démonstration de la supériorité militaire ou le harcèlement de l'ennemi peuvent suffire à rompre sa résistance et donc, à atteindre les objectifs de la guerre.

Dans l'état actuel, les actions dans les milieux stratégiques que sont le domaine spatial et le cyberespace gardent un rôle subsidiaire au côté de la guerre terrestre, maritime et aérienne. La confrontation armée demeure le centre de la guerre, mais nous constatons une explosion de l'utilisation par les États de moyens indirects pour affaiblir sans combattre.

II. L'analyse des conflits armés sous la perspective des penseurs de la guerre

En parallèle de l'apparition de nouveaux milieux stratégiques, la Guerre a évolué pour laisser place à des conflits persistants de relativement basse intensité. Pour autant, les guerres conventionnelles entre États n'ont pas complètement disparu, laissant planer le doute sur un éventuel retour de la guerre de haute intensité.

Mutations des enjeux doctrinaux et des conditions de victoire

L'apparition de l'arme nucléaire et la criminalisation de la guerre par le droit international ont augmenté les risques potentiels des conflits inter-étatiques de manière disproportionnée par rapport aux bénéfices possibles. Ainsi, la grande guerre entre États est devenue synonyme d'anéantissement ou, en tout cas, d'isolation politique. Dès lors, l'utilisation de la guerre comme « continuation de la politique par d'autres moyens » est-elle encore possible ?

[20] CLAUSEWITZ Carl, *On War*, Oxford, Oxford University Press, 2007, p.32.
[21] *Ibid*, p.39.

En réalité, ces évolutions ont davantage transformé les méthodes d'actions des États que supprimé l'utilisation de la guerre comme moyen au service de fins politiques. Ainsi, les États sont devenus plus hésitants à participer de manière transparente et ouverte à des conflits armés contre d'autres États, préférant agir de manière suffisamment détournée pour pouvoir laisser des doutes quant à leur participation dans le conflit. Déjà durant la guerre froide, l'absence d'affrontement direct entre les deux superpuissances avait laissé place à des conflits *proxy*, dans des territoires tiers. La guerre en Ukraine a entériné le concept de *guerre hybride*. Selon Franck G. Hoffman, cette dernière peut être définie comme une guerre « incorporant un éventail complet de modes différents de mener la guerre, parmi lesquelles des capacités conventionnelles, des tactiques et formations irrégulières, des actes terroristes incluant une violence et une coercition indiscriminée, et du désordre criminel. »[22] Sans doute, de telles méthodes ne sont pas nouvelles, poussant certains auteurs à critiquer l'utilité du concept[23]. Ainsi, Sun Tzu différenciait les forces normales (ou « directes ») des forces extraordinaires (ou « indirectes ») qui participent à la bataille[24]. Certains y voient déjà les premières lignes du concept de guerre hybride, mêlant forces conventionnelles et irrégulières.

Si la guerre hybride est ancienne, la nouveauté réside dans la proportion qu'ont prise les forces irrégulières par rapport aux forces conventionnelles. En 2014, le général russe Valerii Guerasimov confirmait l'importance grandissante des méthodes non militaires dans la réalisation de buts politiques et stratégiques ; précisant que, « dans de nombreux cas, elles ont même surpassé de manière significative la puissance des armes en termes d'efficacité. »[25] Selon la « Doctrine Guerasimov », les modes d'action asymétriques permettent de

[22] HOFFMAN Franck G., *Conflict in the 21st Century : The Rise of Hybrid Wars*¸ Arlington, Potomac Institute for Policy Studies, 2007, p.8.
[23] HENNINGER Laurent, « La "guerre hybride" : Escroquerie intellectuelle ou réinvention de la roue ? », *Revue Défense Nationale,* 2016, Vol. 788(3), pp. 51-55.
[24] SUN Tzu, *op.cit.*, p.92.
[25] GUERASIMOV Valerii, « Tsennost' Naouki v Predvidenii », *Voenno-Promyshlennyi Kur'er*, 26 février 2013.

compenser la supériorité d'un ennemi. En particulier, l'utilisation du « potentiel contestataire » de la population est un moyen de diviser l'ennemi en créant un front intérieur permanent, comme c'est le cas en Ukraine. De la même manière, Sun Tzu soulignait l'importance d'épuiser l'ennemi en le gardant occupé en permanence[26] et de l'intimider en lui causant des dommages[27].

Ainsi, l'utilisation de modes d'action asymétriques permet d'affaiblir l'ennemi jusqu'à remporter la décision politique. Ces modes d'action limitent également les possibilités de mise en cause de la responsabilité des États, lesquels ont l'opportunité de rester anonymes en déplaçant le conflit dans le cyberespace, ou bien peuvent se prévaloir de la légitimité potentielle du mouvement protestataire sur lequel ils appuient leurs actions. Ainsi, les mouvements séparatistes en Abkhazie ou en Ossétie du Sud ont préexisté à l'intervention russe et n'ont qu'été nourris par celle-ci. En Crimée, en revanche, la Russie a été plus proactive, s'appuyant sur de simples velléités et non sur des contestations réelles et actives.

En conséquence de la montée en puissance des méthodes asymétriques, les menaces principales sont moins des confrontations armées avec d'autres États que des menaces non conventionnelles et transnationales qui touchent l'État de l'intérieur : le terrorisme, la désinformation, la cyberguerre ou encore l'instrumentalisation de mouvements protestataires. Ces méthodes jouent sur les tensions internes dans le but de les accroitre et de provoquer une paralysie de l'État. De cette manière, c'est directement la volonté politique qui est ciblée, sans passer par la confrontation militaire.

En France, cette nouvelle réalité a été prise en compte en 2008 dans le Livre Blanc sur la défense et la sécurité : « La distinction traditionnelle entre sécurité intérieure et sécurité extérieure n'est plus

[26] SUN TZU, *op.cit.*, p.114.
[27] *Ibid*, p.113.

pertinente »[28]. En effet, les menaces auxquelles sont confrontés les États sont permanentes et non limitées à un champ de bataille, créant une situation ou la paix n'est jamais absolue et contraignant les États à adapter leur stratégie de défense, soit à travers la prévention, par exemple à travers d'autres moyens non militaires comme la régulation des flux d'information et de personnes, soit par des représailles militaires, économiques ou autres. Ainsi, la lutte contre ces moyens de guerre irrégulière a lieu en prévention ou en réaction à l'attaque ; le combat n'est plus, comme l'affirmait Clausewitz, « le seul principe en vigueur parmi les multiples activités qui constituent la guerre »[29].

En dehors de leur territoire, les opérations des États incluent rarement un affrontement avec un autre État, mais ont plutôt pour but le soutien à des mouvements révolutionnaires, la stabilisation d'un État ou la contre-insurrection. Ainsi, le recours à la force armée demeure possible et s'observe principalement dans des opérations à dominante aérienne, comme en Libye en 2011. Ces opérations demeurent basées sur la doctrine de Douhet, selon laquelle celui qui domine les airs obtient la victoire[30]. Pourtant, le développement du droit international a rendu inacceptable l'absence de discrimination entre cibles militaires et populations civiles. Ainsi, avec le développement de la technologie, la mission donnée à l'aviation d'infliger un maximum de dommage dans un temps le plus court possible a laissé place au concept de « frappes chirurgicales », qui visent la destruction de cibles stratégiques tout en diminuant le nombre de victimes civiles. Pourtant, l'utilisation de la doctrine de Douhet est peu adaptée à des contextes de guerre asymétrique, où les combattants ennemis sont diffus et disséminés au milieu de la population et est davantage une conséquence de la réticence des États à déployer des troupes au sol. Ainsi, la lutte contre l'État islamique a été une guerre indirecte pour la coalition internationale,

[28] *Défense et Sécurité Nationale. Le Livre Blanc*, Paris, Odile Jacob, 2008, p.57.
[29] CLAUSEWITZ, *op.cit.*, p.73.
[30] DOUHET Giulio, *op.cit.*, p.25.

dont l'action s'est concentrée essentiellement sur la suprématie aérienne et le soutien aux forces locales.

Dans d'autres cas, les considérations stratégiques continuent cependant de dominer sur les considérations morales : le succès de l'opération française Serval au Mali en 2013 a principalement découlé de la décision d'engager les troupes françaises au sol, lesquelles sont plus adaptées à la contre-insurrection.

Vers un retour à la guerre de haute intensité et une résurgence des penseurs classiques ?

En dehors de Sun Tzu, qui mettait en avant l'importance de l'information, des stratégies indirectes et de la dissimulation, les penseurs de la stratégie classiques trouvent peu d'applicabilité face aux méthodes de guerre hybride. Pourtant, la résurgence des politiques de puissance dans certains États, telles la Russie, la Turquie ou la Chine, pousse à se questionner sur le potentiel retour de la guerre de haute intensité. Par guerre de haute intensité, c'est en réalité la guerre conventionnelle entre grands États qui est envisagée, soit un conflit symétrique utilisant tout le panel de méthodes et d'outils disponibles pour mener l'affrontement. En effet, plusieurs puissances révisionnistes se sentant humiliées ou lésées par l'Histoire mettent leurs moyens en œuvre pour formater une prise de conscience d'un destin national fantasmé.

Ainsi, en septembre 2020, le Président turc Erdogan affirmait le pouvoir de la Turquie de « déchirer les cartes et documents immoraux imposés par d'autres »[31]. Un mois plus tard, le même président turc soutenait activement l'attaque azérie contre les Arméniens du Haut-Karabakh, participant à changer par la violence un *statu quo* qui existait depuis 1994. De la même manière, les ambitions territoriales chinoises

[31] "Turkey Raises Rhetoric in Greece Standoff Ahead of Military Drill", *France 24*, 06 septembre 2020.

en mer de Chine et la militarisation croissante de la zone ont permis à cette dernière d'accroitre lentement son contrôle sur cette zone. Enfin, l'annexion de la Crimée par la Russie en 2014 a également prouvé que cette dernière était prête à utiliser la force armée pour redessiner les cartes. Jusqu'alors, la Russie s'était contentée de former des relations de patronage avec les régions séparatistes qu'elle soutenait, sans aller jusqu'à des transferts de territoires à son bénéfice. Pour autant, cela ne signifie pas que la Crimée soit devenue la nouvelle norme de l'action russe ; elle apparaît au contraire comme une exception. L'Ossétie du Sud n'a jamais été annexée, malgré la volonté exprimée de cette dernière de rejoindre la Russie. De même, l'action de la Russie dans l'est de l'Ukraine consiste à maintenir un conflit de basse intensité et non à mettre tous ses moyens en œuvre pour obtenir une victoire dans la région.

Clausewitz met en avant la nécessité d'une forme de proportionnalité entre les moyens mis en œuvre et les fins politiques[32]. Ainsi, la stratégie hybride telle que mise en œuvre dans l'est de l'Ukraine suffit à atteindre les objectifs actuels de la Russie : créer un danger permanent pour l'intégrité territoriale de l'Ukraine qui la pousse à ignorer temporairement voire à approuver l'annexion de la Crimée ou bien accepter d'autres concessions. Pour autant, cela signifie que si les fins politiques de la Russie évoluent pour inclure une annexion réelle de l'est de l'Ukraine, l'intensité des moyens mis en œuvre augmentera. Cette possibilité est facilitée par la distribution de passeports russes dans le Donbass depuis 2019[33] : une telle politique a déjà été mise en œuvre par la Russie dans d'autres conflits territoriaux, notamment en Géorgie ou « la protection de la vie et de la dignité des citoyens russes, ou qu'ils soient » [34] était l'un des prétextes à l'intervention armée de 2008.

[32] CLAUSEWITZ, *op.cit.*, p.34.
[33] "Pochti 530 Tys. Zhitelei Donbassa Poluchili Rossiiskoe Grazhdanstvo v Uproshchennom Poriadke", *TASS*, 02 mai 2021;
[34] "Interv'iu Dmitriia Medvedeva Rossiiskim Telekanalam", *Kremlin*, 31 août 2008.

Le risque d'une escalade et d'une nouvelle guerre de haute intensité n'est donc pas à exclure alors que la force est utilisée de manière croissante comme moyen de régler les conflits. Les quantités de matériels russes présents sur l'exercice Zapad-2021 ont récemment confirmé la question de la masse et de son retour, ce qui pourrait réhabiliter la pensée de Jomini. Pour autant, si guerre de haute intensité il y a, il est peu probable que celle-ci engage de manière directe des États nucléarisés : Par principe, la guerre « clausewitzienne » ne connaît pas de limite à l'utilisation de la force[35].

Déjà, les affrontements de 2020 au Haut-Karabakh ont montré que la guerre entre États demeure possible et ce, sans nécessairement faire l'objet d'une réaction des grandes puissances. Il est cependant difficile de parler de guerre symétrique dans ce cas précis du fait de la disproportion de moyens aux mains des Azéris et de la présence de leur allié turc. Pour autant, il s'agissait bien d'une guerre ayant pour but d'emporter la décision politique par la destruction de l'adversaire en faisant appel à tous les moyens disponibles : des blindés, la cyberguerre, des drones pour l'Azerbaïdjan, la mobilisation générale pour l'Arménie, etc. Certains auteurs avaient prédit depuis presque vingt ans qu'une croissance économique de l'Azerbaïdjan lui ferait inévitablement considérer la conquête militaire des territoires du Haut-Karabakh[36]. Depuis l'arrivée au pouvoir d'Ilham Aliyev en 2003, les dépenses militaires de l'Azerbaïdjan avaient augmenté de manière continue jusqu'en 2014, ou elles avaient atteint un pic de plus de trois milliards de dollars, puis à nouveau de 2016 à 2020[37]. Une action préventive était donc possible de la part de l'Arménie ou du reste de la communauté internationale : en d'autres termes, « attaquer la stratégie de l'ennemi »[38]. La difficulté première réside donc dans l'anticipation des guerres de haute intensité ; savoir quand l'ennemi ne perçoit plus la

[35] *Ibid*, p.15.
[36] DE WAAL Thomas, *Black Garden. Armenia and Azerbaijan through Peace and War*, New York et Londres, New York University Press, 2003, p.278.
[37] "Military Expenditure Database", *Stockholm International Peace Research Institute*, 2021.
[38] SUN Tzu, *op.cit.*, p.77.

négociation comme une solution envisageable et se prépare à l'offensive armée.

Les penseurs classiques de la stratégie ont écrit, en fonction de leur époque, sur la guerre terrestre, maritime ou aérienne. En dehors de ces milieux stratégiques spécifiques, il semblerait que seuls les éléments les plus généraux de leur pensée soient restés pertinents, comme la question de la sélection des cibles stratégiques ou encore la proportionnalité entre moyens mis en œuvre et fins politiques recherchées. Dans un contexte géopolitique où la guerre entre États peut représenter un coût sacrificiel à travers la destruction nucléaire ou simplement l'isolation politique, les guerres ont évolué pour laisser une place plus importante à la dissimulation ou la manipulation. Ainsi, alors que certains auteurs ont perdu de leur pertinence avec la montée en puissance des moyens de guerre asymétriques, Sun Tzu est devenu plus actuel que jamais, sa stratégie visant la victoire sans l'affrontement. De même, les nouveaux moyens au service des États, en particulier les possibilités offertes par le cyberespace, facilitent la dissimulation et permettent de causer des dommages aux autres États de manière anonyme.

Pourtant, le retour des politiques de puissance et des ambitions territoriales de certains États pousse à se questionner sur un éventuel retour de la guerre de haute intensité. Si de telles guerres ont peu de chance de concerner directement de grands États nucléarisés, la guerre entre l'Arménie et l'Azerbaïdjan a prouvé qu'un affrontement relativement symétrique entre États était possible avec, potentiellement, le soutien militaire de puissances plus importantes ; en l'occurrence, la Turquie. Si les guerres usant de moyens asymétriques restaient la norme, le succès incontesté de l'offensive azérie pourrait servir de modèle à d'autres guerres similaires ; le conflit au Haut-Karabakh ayant prouvé que la force militaire peut être plus efficace que la négociation et que son utilisation n'est pas nécessairement sanctionnée.

Bibliographie

Agence France Presse, « L'Inde annonce avoir détruit un satellite en orbite avec un missile », *Le Monde*, 27 mars 2019.

Agence France Presse, "Turkey Raises Rhetoric in Greece Standoff Ahead of Military Drill", *France 24*, 06 septembre 2020.

BOYER Bertrand, *Guérilla 2.0. Guerres irrégulières dans le* cyberespace¸ Paris, Editions de l'Ecole de Guerre, 2020, 352p.

CLARKE Richard A., KNAKE Robert K., *Cyber War : The Next Threat to National Security and What to Do About It*, New York, HarperCollins e-books, 2010,140p.

CLAUSEWITZ Carl, *On War*, Oxford, Oxford University Press, 2007, 284p.

CORBETT Julian, *Principles of Maritime Strategy*, New York, Dover Publications, 2012, 338p.

DE WAAL Thomas, *Black Garden. Armenia and Azerbaijan through Peace and War*, New York et Londres, New York University Press, 2003, 337p.

DOLMAN Everett, *Astropolitik. Classical Geopolitics in the Space Age*, Londres, Routledge, 2005, p.208.

DOUHET Giulio, *The Command of the Air*, Maxwell, Air University Press, 2019, 362p.

GUERASIMOV Valerii, « Tsennost' Nauki v Predvidenii », *Voenno-Promyshlennyi Kur'er*, 26 février 2013.

HENNINGER Laurent, « La "guerre hybride" : Escroquerie intellectuelle ou réinvention de la roue ? », *Revue Défense Nationale*, 2016, Vol. 788(3), pp. 51-55.

HERZOG Stephen, « Revisiting the Estonian Cyber Attacks : Digital Threats and Multinational Responses », *Journal of Strategic Security*, 2011, Vol. 4(2), pp. 49-60.

HOFFMAN Franck G., *Conflict in the 21st Century : The Rise of Hybrid Wars*¸ Arlington, Potomac Institute for Policy Studies, 2007, 72p.

JEWKES S., POLITYUK P., VUKMANOVIC O., « Ukraine Power Outage was a Cyber-Attack : Ukrenergo », *Reuters*, 18 janvier 2017.

JOMINI Antoine Henri, *The Art of War*, Kingston, Legacy Books Press, 2008, 330p.

KOLIOPOULOS Constantinos, PLATIAS Athanassios,*Thucydides on Strategy: Grand Strategies in the Peloponnesian War and Their Relevance Today*, Oxford, Oxford University Press, 2017, 224p.

KREPINEVICH Andrew F., *Cyber Warfare. A "Nuclear Option" ?*, Center for Strategic and Budgetary Assessment, 2012, Washington, 85p.

MAHAN Alfred Thayer, *The Influence of Sea Power Upon History. 1660-1783*, Boston, Little, Brown and Company, 1890, 557p.

"Pochti 530 Tys. Zhitelei Donbassa Poluchili Rossiiskoe Grazhdanstvo v Uproshchennom Poriadke", *TASS*, 02 mai 2021.

RID Thomas, "Cyber War Will Not Take Place", *Journal of Strategic Studies*, 2012, Vol.35(1), pp. 5-32.

SUN Tzu, *The Art of War*, Londres, Oxford University Press, 1963, 197p.