L'émergence des menaces hybrides: vers une autre transformation de la guerre?

cahier de la pensée mili-Terre

le Chef de bataillon Cédric LE BIGOT

Publié le 22/07/2018

Histoire & stratégie

Une tendance marquante de ces dernières années est l'effacement progressif des distinctions traditionnelles entre guerre et paix, entre acteurs étatiques et non étatiques; mais aussi entre des modes d'action très différents: guerre conventionnelle, insurrectionnelle, cybercriminalité, terrorisme et crime organisé. Ces nouvelles menaces, connues sous le nom de menaces hybrides, multiples et adaptatives, sont amenées à se développer sur le moyen comme sur le long terme. Les conséquences possibles pour nos forces armées sont nombreuses en termes de capacités requises, modes d'action et investissement technologique.

«À l'avenir, la guerre ne sera pas le fait des armées, mais celui de groupes, appelés aujourd'hui terroristes, guérilleros, bandits, voleurs de grand chemin, mais ils chercheront sans aucun doute des titres plus officiels. Plus charismatiques qu'institutionnels, leurs organisations s'appuieront davantage sur des fidélités cimentées par le fanatisme et l'idéologie que sur le professionnalisme».

Martin Van Creveld,

«La transformation de la guerre».

En s'attaquant aux fondements de nos sociétés, les menaces hybrides inquiètent par leurs formes multiples et leur caractère insaisissable. En permanente adaptation, tirant profit des évolutions technologiques, elles se développent insidieusement en poursuivant des objectifs variés : pouvoir, profit, religion… Face à un tel adversaire, souvent difficile à identifier et à prévoir, les états se trouvent particulièrement exposés et souvent impuissants. En outre, l'estompement des frontières comme barrières aux menaces a accentué le sentiment d'insécurité sur le territoire national. Les implications pour nos forces armées sont nombreuses en termes de capacités requises, de doctrine et d'investissements technologiques.

Une menace en développement, qui recouvre plusieurs champs d'application

- **Genèse du concept**

Le concept de menaces hybrides a émergé durant la dernière décennie parmi de nombreux think-tanks américains. Dérivé du concept d'irregular threat, **il décrit une forme émergente de menaces, dans laquelle des acteurs principalement non-étatiques mettraient en œuvre une combinaison de moyens à la fois cinétiques (guerre conventionnelle, asymétrique, crime organisé) et non cinétiques (actions subversives, politiques, sociales).** Depuis 2010, l'OTAN s'est emparé du concept[1], dans l'objectif de développer une stratégie efficace et des applications concrètes en termes de modes d'action et de capacités requises.

- **Un adversaire hybride par ses procédés,…**

La complexité de ces menaces réside d'abord dans la grande variété de leur champ opératoire. Si la diversité des situations rencontrées et des conflits actuels (terrorisme, piraterie, contre-insurrection, cybercriminalité) n'est pas nouvelle en soi, **la menace principale réside dans la possibilité pour un adversaire de choisir et de combiner des actions (conventionnelles, asymétriques, politiques…) pour la poursuite d'un objectif à moyen ou long terme**. Ces procédés, utilisés et choisis à dessein par un même acteur, pourraient avoir un effet multiplicateur d'efficacité, car opérant dans des domaines très différents (militaire, économique, social, industriel…). Car le concept de menaces hybrides regroupe également les actions non purement militaires, telles que les opérations d'information ou d'influence, la cybercriminalité ou les pressions économiques. Enfin, l'hybridation des procédés est renforcée par une capacité d'adaptation permanente chez l'adversaire, peu contraint par des considérations doctrinales ou éthiques.

- **…. par sa nature et sa zone d'action,…**

L'aspect tentaculaire de ces menaces doit par ailleurs beaucoup à leur caractère transnational, renforçant leur aspect insaisissable. Surtout, l'ennemi futur sera moins un État qu'un groupe d'individus, s'affranchissant des frontières et se coordonnant grâce aux nouveaux moyens de communication. **De fait, l'origine des menaces, entre acteurs étatiques et non-étatiques, est parfois plus complexe à caractériser.** À titre d'exemple, les cyber-attaques se situent typiquement dans une zone grise entre la paix et la guerre, et la difficulté à en déterminer l'origine avec certitude brouille les cartes entre acteurs étatiques et non étatiques. Facteur aggravant, les zones de conflits des «guerres hybrides» de demain seront majoritairement des zones urbanisées, souvent côtières, et abritant une forte activité économique. Ces lieux d'affrontement, appelés contested zones dans la doctrine américaine, représentent un milieu idéal pour le développement de modes d'action hybrides, tout en rendant particulièrement complexe une réponse de type conventionnelle, même dotée d'une technologie développée.

- **…qui s'immisce au cœur de nos sociétés.**

Faire le portrait d'un ennemi aux multiples visages n'est pas sans difficulté, en particulier lorsque ce dernier s'attaque aux fondements, aux valeurs, et aux caractéristiques

marquantes de nos sociétés: médiatisation, libertés individuelles, judiciarisation, interconnexion et interdépendance. En s'attaquant à la population et aux institutions, en prenant pour cibles nos centres de gravité, souvent par une approche indirecte qui est le propre de l'asymétrie, ces groupes sont en position d'influer notablement sur l'opinion publique, voire sur les autorités politiques visées. Face à un ennemi s'affranchissant de toutes les règles du droit international, les parades sont limitées et le niveau de vulnérabilité est, de fait, accentué. Dans ce contexte, les frontières ne constituent plus des lignes de protection naturelles, car nos sociétés globalisées sont de plus en plus tributaires des flux de personnes, de biens et d'information. Cette dépendance nous rend plus exposés aux menaces pesant sur ces flux, notamment dans des zones difficilement contrôlables: zones maritimes ou aériennes internationales, espace ou cyberespace.

Hybridation de la menace: deux cas concrets

- **Le Hezbollah, un quasi État aux modes d'action multiples**

Acteur non-étatique, le Hezbollah a atteint aujourd'hui une capacité à contraindre et influencer proche de celui des États, se dotant de moyens militaires et de technologies rendus aujourd'hui plus accessibles. Cet «État dans l'État» s'affirme selon plusieurs caractéristiques: la maîtrise d'un territoire (le Liban sud), des relations interétatiques (Syrie et Iran), le contrôle de la vie civile (social, éducatif et santé), des forces militaires et un contrôle opérationnel (milice armée et structurée), le tout autour d'une sacralisation de ses chefs religieux. Agissant tour à tour dans les sphères politique, militaire et sociale, il a indéniablement un caractère hybride. À l'été 2006, il a clairement démontré sa capacité à repérer et cibler les vulnérabilités de l'État d'Israël, menant notamment une «techno-guérilla» et dépassant ses capacités classiques de combat (utilisation d'engins explosifs improvisés contre les Merkava, combattants dotés de moyens de protection et de vision nocturne modernes, de dispositifs de réduction de signature infrarouge et de reconnaissance par drones «Mirsad»). **Son arsenal développé et ses capacités d'adaptation lui ont permis d'évoluer intelligemment pour maintenir une pression constante sur Israël**[2]**.** Se posant en protecteur d'une population injustement opprimée, il a gagné le soutien local de la population et d'une partie de l'opinion publique internationale. Par ailleurs, les liens avérés avec l'Iran et la Syrie ont donné à ce groupe religieux une dimension internationale.

- **Le Mexique ou la notion de «**criminal insurgency**» sur fond de ramification transnationale**

L'application au cas mexicain du caractère multiple des menaces décrites précédemment ne fait aucun doute. Les opérations anti-narcotiques en Colombie et dans d'autres zones d'Amérique du Sud et Centrale ont entraîné un déplacement des activités criminelles au Mexique, où de nombreux cartels ont trouvé un véritable sanctuaire. L'accroissement de ces activités illicites a généré des revenus estimés entre 19 et 29 milliards de dollars, essentiellement centrés sur les activités criminelles transfrontalières avec les États-Unis[3]. Les cartels luttant entre eux pour le contrôle des territoires d'une part, et compte tenu du niveau de violence à l'égard de la population et des autorités d'autre part, la menace se situe clairement à la confluence du crime, du terrorisme et de l'insurrection. Les administrations locales, dépassées par l'ampleur et la violence du phénomène, ont dû faire face à la pression de ces «insurgés criminels», désireux de

prendre le dessus sur les juridictions locales (corruption, menace…). Malgré les 45.000 soldats mobilisés par le président Calderon pour lutter contre ce fléau, le bilan est particulièrement lourd: 45.000 meurtres perpétrés depuis décembre 2006, plus de 3.600 enlèvements depuis 2009, et 120.000 personnes ayant fui leur domicile. L'insécurité au Mexique est devenue un problème national et **50% du territoire et de la population sont hors du contrôle du gouvernement.**

Comment expliquer que le Mexique, qui n'est pas un état défaillant, éprouve autant de difficultés à répondre à cette menace? Un élément de réflexion réside dans le caractère régional des réseaux criminels colombiens, en particulier au Guatemala, au Honduras et bien-sûr aux États-Unis où une contagion du phénomène est à craindre. **Mais un autre aspect de la menace inquiète les acteurs de la scène internationale: il s'agit des liens entre les cartels et d'autres acteurs internationaux.** En effet, les connexions des cartels sud-américains avec d'autres acteurs non-étatiques tels que le Hezbollah[4], ou étatiques comme l'Iran[5], ont récemment été mis à jour. Cet aspect du problème révèle toute la complexité du cas mexicain: lutter contre un ennemi intérieur, alors même que ce dernier peut bénéficier d'un soutien étendu et de filières pour le développement des trafics, notamment parce que la mondialisation a permis l'accroissement des flux financiers. L'aspect tentaculaire de ces réseaux et l'hybridation de l'ennemi (mélange de groupes criminels, terroristes, soutenus par des États tiers) sont particulièrement révélateurs des nouveaux types de menaces, voire d'une transformation de la guerre.

Quelles impacts sur les armées?

- **Redécouvrir l'ennemi: la pertinence de l'approche globale**

L'émergence des menaces hybrides vient révolutionner les modes de pensée traditionnels tout en donnant raison aux partisans de l'approche globale. En effet, le spectre large des menaces les rendant difficilement prévisibles et lisibles, les parades sont complexes à mettre en œuvre car elles requièrent la coordination d'une grande variété d'acteurs dans de nombreux domaines: économique, gouvernance, État de droit… **L'analyse des menaces doit, en outre, considérer l'ennemi comme un système organisé**[6]. Un des principaux enseignements du conflit afghan fut la nécessaire coopération entre secteurs civil et militaire, ainsi que l'établissement d'une meilleure communication et d'une confiance mutuelle, notamment entre les différentes autorités. Cependant, l'unité d'effort, seul gage du succès, requiert idéalement une unité de commandement. Cette dernière est souvent difficilement réalisable car rejetée par certains acteurs comme les ONG, qui craignent de voir remise en cause leur neutralité. **En définitive, si l'approche globale constitue une réponse possible pour contrer les menaces hybrides, la variété des modes d'action possibles implique une convergence de vue et la mise en œuvre de lignes d'opérations englobant tous les domaines (sécuritaire, politique, économique, social**…). Dans l'accomplissement de sa mission, le chef militaire de demain devra plus que jamais prendre en compte ces différents aspects, les connaître et être en mesure d'intégrer des acteurs civils et gouvernementaux dans le cadre de la planification des ses actions. Il devra également être conscient qu'il ne sait pas tout, qu'une part d'incertitude subsiste compte tenu de la complexification des

menaces évoquées précédemment, et ce en dépit des efforts tentés pour réduire le brouillard de la guerre[7].

- **La nécessaire adaptation des forces armées**

Face à un adversaire possédant des modes d'actions multiples, il est impératif de conserver nos capacités d'action dans un spectre très large: combat de haute intensité, contre-insurrection, maîtrise de la violence, tout en restant prêts à affronter des actions terroristes, criminelles ou à base de cyberattaques. En d'autres termes, **la flexibilité et la réversibilité de nos forces armées sont essentielles pour répondre à un ennemi insaisissable et en permanente adaptation**. La prise en compte par les armées de ces nouveaux types de conflits doit nécessairement englober de nombreux domaines, tel que le corpus doctrinal, la formation ou l'entraînement des forces, à l'image des initiatives prises par le corps des Marines pour entraîner ses chefs militaires à «réagir à l'inconnu dans un environnement complexe et hostile»[8]. Le succès face aux menaces hybrides passe également par une meilleure prise en compte du renseignement et une adaptation de nos procédures, notamment pendant la phase de planification[9]. Par ailleurs, compte tenu de la généralisation des technologies, l'adversaire de demain sera en mesure d'opérer avec un niveau de sophistication inégalé jusqu'à présent. Le taliban afghan et ses moyens rudimentaires ne seront qu'un lointain souvenir: l'insurgé de demain mettra en œuvre des brouilleurs, des drones et des robots du champ de bataille, tout en étant soutenu et financé par des activités criminelles (kidnapping, trafics) ou des États tiers. **Dans ce contexte, il sera nécessaire de conserver une avance technique significative, sans toutefois tomber dans l'illusion de la suprématie technologique[10]**. Dans ce domaine, la coopération, voire la mutualisation au niveau international semble inévitable compte tenu du contexte budgétaire actuel. Le maintien à flot d'une industrie de défense performante, tant au niveau national qu'au niveau européen est également indispensable pour maintenir cette avance technologique. Par ailleurs, conserver des moyens en mode dégradé, moins sophistiqués mais aussi moins vulnérables, pourrait permettre de conserver une forme de résilience face à la menace d'attaques électroniques.

Les attentats du 11 septembre 2001 ont mis à jour une réalité complexe: celle d'une situation à cheval entre guerre et paix, dans laquelle la suprématie technologique n'est plus un facteur suffisant de succès. La mondialisation, l'accessibilité des technologies et la perméabilité des frontières ont révélé l'émergence d'un ennemi difficilement perceptible et utilisant des modes d'action multiples. Cet ennemi n'a rien à voir avec l'adversaire traditionnel d'hier, bien défini et opérant selon une doctrine connue. Il conviendrait donc de revoir notre grille de lecture de l'ennemi, en particulier en poursuivant le développement d'outils d'analyse systémique et d'aide à la décision[11]. Prendre en compte l'ensemble du spectre des menaces requiert par ailleurs une coopération accrue qui dépasse le cadre des forces armées, notamment en matière de renseignement. L'effacement progressif des frontières comme barrières aux menaces a accru la vulnérabilité du territoire national. Dès lors, l'effort doit également être porté sur le maintien d'un niveau élevé de flexibilité et de réversibilité des forces armées, tout en accentuant le développement de modes d'action adaptés.

Compte tenu de cette évolution, un enjeu majeur réside donc dans l'anticipation de ces nouvelles menaces sur le moyen comme sur le long terme. À titre d'exemple, l'Alliance atlantique a publié en 2009 une étude importante sur quatre scenarii futurs possibles[12]:

- le premier d'entre eux, la face sombre de l'exclusivité, décrit une situation ou l'équilibre interne des nations et l'ordre international lui-même sont compromis par une mondialisation mal maîtrisée;
- dans le deuxième, la stabilité trompeuse, les préoccupations démographiques accaparent en interne l'attention des États, les rendant vulnérables à une surprise géopolitique;
- le troisième scénario, le choc des modernités, imagine la poursuite de la globalisation d'un monde développé interconnecté, menacé à ses marges par des régimes ne partageant pas ses valeurs;
- enfin, la nouvelle politique de puissance, mettant l'accent sur l'émergence de nouveaux acteurs de premier plan, imagine la quête incertaine d'un nouvel équilibre international sur fond de compétition pour les ressources.

Une telle modélisation, fondée sur des conséquences logiques d'évolutions souvent déjà à l'œuvre, doit être considérée comme une étape vers le développement d'outils censés «répondre au plus large spectre des défis à venir»[13]. Les révolutions arabes de 2011, surprise stratégique non moins prévisible a posteriori que ne l'était celle de 2001, montre que ces outils n'ont pas encore atteint leur seuil d'efficacité ou sont inadaptés. L'effort des États comme des organisations internationales devrait se concentrer sur cette fonction d'anticipation, condition sine qua non de notre faculté d'adaptation face aux menaces hybrides.

Bibliographie indicative liée à l'article:

- «Le contexte stratégique de l'OTAN à l'horizon 2030», du Général Stéphane ABRIAL
- "The Hybrid threat: crime, terrorism and Insurgency in Mexico", Center for Strategic Leadership (US ARMY WAR COLLEGE), Dec 2011
- "Irregular warfare and hybrid threats", Joint Irregular Warfare Center
- Training Circular 7-100: Hybrid threat, US ARMY
- "Conflict in the 21st Century: the rise of hybrid wars", Frank Hoffman, Potomac Institute for Policy Studies

[1] ACT (Allied Command Transformation) a initié le projet CHT (Countering Hybrid Threat)

[2] Le Hezbollah face aux forces armées, cahier de la Recherche, CDEF, mars 2009

. La guerre de juillet, cahier du RETEX, CDEF, sept 2006

[3] Source: Centre for Strategic Leadership (US ARMY WAR COLLEGE), Dec 2011

[4] Selon plusieurs experts, le Hezbollah aurait forgé un partenariat avec certains cartels de la drogue au Mexique. Le groupe recevrait un soutien financier et une protection des cartels en échange de l'expertise du Hezbollah.

[5] En octobre 2011, la justice américaine a arrêté deux ressortissants iraniens accusés de tentative d'assassinat de l'ambassadeur d'Arabie saoudite aux États-Unis. Les iraniens auraient tenté d'agir par l'intermédiaire d'un groupe de narcotrafiquants mexicains.

[6] À l'instar de la phase de CPOE (Comprehensive Preparation of the Operational Environment) qui initie la séquence de planification de l'OTAN (COPD)

[7] Notamment dans le domaine de l'Information Dominance

[8] Aux Etats-Unis, le Joint Irregular Warfare Center (JIWC) a été créé pour répondre à ce vide doctrinal

[9] En 2011, une conférence de l'OTAN s'est réunie à Tallinn pour étudier et développer une approche commune civilo-militaire des menaces hybrides

[10] Depuis la guerre en Irak en 2003, de nombreux stratèges américains considèrent que l'impact de la révolution dans les affaires militaires (RAM) a été clairement surestimée (Ref: Potomac Institute for Policy Studies)

[11] Notamment au travers d'outils de type recherche opérationnelle

[12] ACT: Multiple Futures Project: navigating towards 2030

[13] «Le contexte stratégique de l'OTAN à l'horizon 2030», du Général ABRIAL

Saint-cyrien de la promotion de «La France combattante» (1997–2000), le Chef de bataillon Cédric LE BIGOT a servi à la 785ème compagnie de guerre électronique, puis au 54ème régiment de transmissions. Il a ensuite occupé les fonctions de chef de centre opérations de guerre électronique et d'officier traitant au sein du G2 du corps de réaction rapide France. Après avoir été stagiaire de la 125ème promotion du cours supérieur d'état-major, il suit actuellement la scolarité de l'École de guerre.

Titre : L'émergence des menaces hybrides: vers une autre transformation de la guerre?

Auteur(s) : le Chef de bataillon Cédric LE BIGOT

Date de parution : 10/07/2018