LE RUBICON

L'OTAN et les opérations multidomaines

Olivier Rittimann | 31 août 2023 | ARTICLES |

Alors qu'à l'époque de la Guerre froide, la doctrine de l'OTAN consistait à encaisser le coup sur la ligne de front et à dégrader les échelons successifs ennemis (*Air Land Battle*), en distinguant ainsi le front, la profondeur et l'arrière, aujourd'hui ces distinctions ont moins de pertinence. Certes, la guerre en Ukraine semble démontrer le contraire, puisque les notions de front, de profondeur et d'arrière y restent d'actualité, mais il s'agit-là d'un conflit qui reste contenu sur un territoire, entre deux puissances qui ne sont pas égales. On y voit effectivement l'utilisation de drones sur fond de guerre de tranchées, mais on n'a pas assisté à une attaque cyber de grande envergure réellement efficace qui aurait paralysé l'un des belligérants ; et il n'y a pas eu de destruction de satellites, comme ce serait vraisemblablement le cas dans un conflit futur entre grandes puissances. Or, les moyens de frappe dans la profondeur ont considérablement accru l'allonge ; les attaques dans le domaine cyber s'affranchissent des notions de distance, de géographie ou de délais ; et la paralysie des communications et des systèmes de positionnement ou d'alerte avancée situés dans l'espace extra-atmosphérique gênera les mouvements.

Nos adversaires potentiels, qu'ils soient russes ou chinois, ont appris en nous regardant faire. La multiplication des opérations extérieures occidentales leur a permis d'étudier nos points forts, mais aussi nos faiblesses, et de chercher ainsi à compenser leurs propres désavantages en tentant d'exploiter ces vulnérabilités. Ainsi, si l'Union soviétique savait parfaitement que la défense de l'Europe reposait en grande partie sur la garantie d'acheminement de renforts transatlantiques, elle n'avait pas les moyens d'interdire l'accès aux ports d'Europe de l'Ouest, contrairement à la Russie qui dispose aujourd'hui d'un large éventail de missiles avec la portée et la précision nécessaires, mais également de la capacité à désorganiser les réseaux essentiellement civils de ces infrastructures, via les attaques cyber. Quant aux Chinois, ils ont étudié en détail l'opération *Desert Shield* puis *Desert Storm*, lors de la première guerre du Golfe, et en ont tiré des enseignements qu'ils ont patiemment assimilés, sur le besoin indispensable des frappes dans la profondeur pour désorganiser le commandement ennemi avant tout déclenchement d'une opération terrestre, sur la nécessité d'interdire l'accès de renforts à la zone des combats, mais en ont aussi déduit que la guerre future ne se limiterait pas aux seules manœuvres militaires ; elle devrait faire appel à tout l'éventail des instruments disponibles pour faire plier l'ennemi.

Lors des opérations en Afghanistan et en Irak, le modèle expéditionnaire américain a été décortiqué, aussi bien par les Chinois

qui l'étudient dans le contexte d'un conflit dans le Pacifique, que par les Russes qui en appliquent les leçons pour leur propre expédition en Syrie en 2015. Ils constatent que les Américains doivent systématiquement projeter leurs forces loin de leurs bases nationales, les acheminer, les assembler, donc disposer de lignes de communication maritimes ou aériennes protégées, de bases et de zones de regroupement (*staging areas*) à l'abri des frappes potentielles ennemies. Tant que le déploiement se faisait pour une opération de gestion de crise, où la supériorité aérienne et navale n'était pas remise en question, le modèle était performant, même s'il était coûteux en matière de ressources. Or, aujourd'hui avec la montée en puissance des capacités chinoises, prévoyant d'interdire l'accès à la zone avec la mise en œuvre de tout un arsenal allant des groupes de porte-avions aux missiles antiaériens à très longue portée, en passant par une aviation de chasse performante et des missiles antinavires, le modèle américain de projection de force trouve ses limites, en particulier face à la Chine, compte-tenue de l'immensité du théâtre d'opérations potentiel dans le Pacifique. En ce qui concerne la Russie, les élongations sont moindres, mais exigent que l'Atlantique nord soit sécurisé, d'où la remise en service aussi bien aux États-Unis qu'à l'OTAN de la 2e Flotte et du commandement interallié de Norfolk.

En outre, le développement ultra rapide de nouvelles technologies bouleverse la notion même de champ de bataille. En effet, l'intelligence artificielle, la nanotechnologie, la biotechnologie, les systèmes autonomes, les essaims de drones, les armes à effet dirigé, voire basées dans l'espace extra-atmosphérique, ou le calcul quantique pourraient révolutionner la façon de faire la guerre sur terre, dans les airs et sur mer. La transition occidentale vers des opérations multidomaines pourrait apporter une réponse à ces défis.

Origine et objectif

Le concept d'opérations multidomaines (*Multi Domain Operations*, MDO) est né aux États-Unis vers 2017, avec le constat que la guerre future n'aurait pas l'aspect du conflit en Afghanistan ou en Irak, compte tenu de la montée en puissance des capacités chinoises, et qu'il faudrait donc dominer les adversaires dans les domaines traditionnels que sont le milieu terrestre, aérien ou maritime, mais aussi assurer la supériorité américaine dans le cyberespace et l'espace extra-atmosphérique. Par conséquent, ce sont ces cinq domaines qu'on englobe dans le concept de multidomaines. On pourrait aussi considérer l'information comme un domaine supplémentaire permettant de façonner le champ des perceptions, mais, à l'heure actuelle, ce ne sont que les cinq mentionnés plus haut qui sont reconnus en tant que tels aussi bien par les États-Unis que par l'OTAN, même si certains Alliés, par exemple la France, définissent également, en sus de ces domaines, les champs informationnel et électromagnétique.

Même si certains prétendent que ce n'est jamais que de l'interarmées avec une touche de ces deux nouveaux domaines, il ne s'agit pas simplement de rajouter le cyber et l'espace aux domaines traditionnels. En fait, le concept est beaucoup plus complexe. L'interarmées, le *Joint*, consiste à synchroniser les activités d'au moins deux composantes, par exemple les forces terrestres et les forces aériennes, sous les ordres d'un commandant interarmées. Les activités de cette force interarmées demeurent toutefois entièrement militaires, même s'il peut y avoir des interactions civilo-militaires prévues dans le plan d'opération ou rendues nécessaires par les effets de l'opération elle-même. Le multidomaine va plus loin, en ce qu'il va chercher à synchroniser ces activités militaires interarmées avec d'autres effets qui, eux, sont principalement dans les mains civiles, le cyber et l'espace, et d'en obtenir l'effet requis, au moment requis.

Il faut pouvoir faire converger les effets de tous les domaines ou d'une combinaison de ces domaines vers une cible, en mettant l'accent sur le domaine plutôt que sur la composante qui en était traditionnellement en charge. Ainsi, le domaine aérien est évidemment affecté par les forces aériennes, mais peut l'être aussi par les forces terrestres ou navales, ou encore le cyber ou l'espace. L'effet recherché peut être obtenu dans la dimension physique, virtuelle ou cognitive. La cible peut donc être matérielle : un aéroport, un dépôt de munitions, une concentration de blindés ; ou immatérielle : un site internet, un auditoire, un public. L'effet obtenu peut être létal : un bombardement, un missile ; ou non létal : la paralysie d'un site internet, la neutralisation d'un nœud ferroviaire, d'un système bancaire, d'un ensemble hospitalier, etc.

L'adaptation technologique

Pour que les effets arrivent en temps, en lieu et en quantité souhaités, tout le cycle d'analyse et de décision – le fameux *OODA (Observe-Orient-Decide-Act) loop* – doit être extrêmement rapide, en tout cas plus rapide que celui de l'adversaire. On devra disposer d'un système qui permette d'intégrer toutes les informations obtenues par tous les capteurs disponibles, d'en effectuer l'analyse et la synthèse au moyen de l'intelligence artificielle pour déterminer lesquelles sont pertinentes, et de présenter ainsi des options aux décideurs.

Il faut pouvoir connecter les différents tuyaux d'orgue résultant des différentes façons de travailler entre les armées au sein d'un pays, ou entre partenaires de coalition. Les différences de culture, de tempo opérationnel, de soutien logistique, de systèmes d'information et de commandement sont déjà difficiles à harmoniser au sein d'un seul pays, comme les Américains peuvent en témoigner, en dépit d'une doctrine *Joint* qui remonte aux années 1990. La difficulté est encore accentuée quand on travaille au sein d'une coalition ou d'une alliance, du fait des disparités entre contributeurs, mais aussi du fait des restrictions dans le partage du renseignement entre coalisés, voire entre Alliés comme le fameux *Five Eyes* qui ne permet le partage de renseignement américain qu'avec les Britanniques, les Canadiens, les Australiens et les Néo-zélandais.

La standardisation des procédures et l'interopérabilité des moyens permettent certes de surmonter quelques obstacles, mais ce qu'il faut à présent c'est une architecture de données et de systèmes qui soit résiliente, réactive et plus rapide que celle dont dispose l'adversaire. C'est d'autant plus urgent que nous entrons à présent dans une phase de compétition stratégique entre grandes puissances. Elle couvait depuis quelques années, mais s'est révélée avec l'invasion russe en Ukraine et la montée en puissance de la Chine, deux défis auxquels l'Occident doit faire face dans l'immédiat pour la Russie et dans un futur proche pour la Chine. En effet, la recette utilisée pour les opérations de gestion de crise qui consistait à établir un réseau où tous les acteurs pouvaient se connecter sans réel risque d'intrusion ou d'interception (type *Afghan Mission Network*) ne suffira pas face à des adversaires disposant des mêmes capacités, voire de capacités plus avancées. La quantité de données échangées dans ce type d'environnement permissif est très élevée, mais n'est pas sujette à des intrusions ou à des attaques et ne demande donc pas de traitement pour l'optimiser. Ce n'est évidemment pas le cas pour un affrontement de haute intensité où la quantité de données doit être réduite, peut être interceptée ou corrompue par un adversaire disposant de capacités équivalentes. Il convient d'optimiser l'information transmise et de s'assurer qu'elle reste protégée pendant sa transmission et qu'elle arrive à son destinataire de manière fiable et rapide. Une des possibilités serait de créer un *Combat Cloud*, un réseau décentralisé, protégé des attaques cyber, collaboratif et partagé entre les domaines terrestre, aérien, naval, cyber et spatial. L'objectif serait de connecter toutes les forces et d'intégrer des plateformes hétérogènes afin de permettre l'échange d'information en temps réel.

Le défi de la définition

L'OTAN s'intéresse traditionnellement, avec quelques années de décalage, aux concepts américains, et MDO ne fait pas exception. Il ne s'agit cependant pas de copier-coller le concept américain, qui n'existe d'ailleurs pas au niveau interarmées, chaque *Service* ayant sa propre interprétation. L'*US Army* le définit comme l'emploi de capacités terrestres et interarmées afin de créer et d'exploiter un avantage relatif pour atteindre des objectifs, défaire les forces ennemies et consolider les acquis au profit du commandant de la force interarmées. L'*US Air Force* définit MDO comme l'acquisition, le fusionnement et l'exploitation de l'information provenant de sources multiples pour l'intégrer dans la planification et l'exécution d'opérations dans le cadre espace-temps requis pour remplir les objectifs du commandeur, en soulignant la nécessité de faire converger les moyens aériens, spatiaux et cyber.

Dans l'Alliance, l'adoption d'un nouveau concept doit faire l'objet d'un consensus des 31 Alliés. Le premier consensus doit porter sur la définition de MDO pour l'OTAN qui n'a adopté, à ce stade, qu'une définition temporaire devant permettre aux intervenants comme le commandement allié pour la transformation ou celui pour les opérations de poursuivre le travail d'étude : « l'orchestration d'activités militaires à travers tous les domaines et les environnements, synchronisée avec des activités non militaires, pour permettre à l'Alliance de délivrer des effets convergents avec la rapidité nécessaire ». Comme l'écrit encore le Centre de guerre interarmées de l'OTAN (Joint Warfare Centre, Stavanger), MDO doit orchestrer ce qui est contrôlé par les militaires et, en collaboration avec un cercle de plus en plus important d'intervenants, synchroniser les activités et les capacités d'autres acteurs qui aident à atteindre l'objectif militaire. Et cette synchronisation doit s'effectuer en permanence afin d'exploiter toutes les opportunités qui se présenteraient, quelle que soit la phase du conflit, et cela du niveau stratégique au niveau tactique.

Le Digital Backbone, la colonne vertébrale numérique de l'Alliance

En mars 2022, le commandement allié Transformation (*Allied Command Transformation*, ACT), en collaboration avec le ministère de la Défense britannique, organisait la première conférence sur le MDO afin d'y voir un peu plus clair dans les travaux qu'il convenait de mener. La conclusion principale était que MDO n'était pas un concept militaire habituel et qu'il devait s'inscrire au sein de l'approche plus large des instruments de pouvoir : diplomatique, informationnel, militaire et économique. La deuxième conclusion insistait sur l'urgence de procéder à la transformation numérique de l'Alliance, chantier qui vivotait depuis une dizaine d'années, sans quoi la démarche n'aurait pas de sens. Il s'agit donc de développer cette architecture numérique, le *Digital Backbone*, qui doit permettre la connectivité sécurisée et rapide entre Alliés, voire partenaires.

Mais la transformation numérique de l'Alliance par la technologie ne sera pas suffisante pour basculer vraiment sur le MDO. Il faut aussi revoir les procédures, former des opérateurs qui comprennent la démarche MDO, jusqu'aux plus bas échelons. Un programme d'éducation et d'entrainement à cette nouvelle « philosophie » va donc devoir être mis sur pied, à la fois par les nations individuellement, mais aussi par l'Alliance qui doit graduellement incorporer le MDO à ses exercices collectifs.

Pour cela, il faudra aussi revoir la façon dont les forces sont organisées : la traditionnelle hiérarchie du stratégique au tactique pourrait faire moins sens et surtout devenir un obstacle à la dissémination rapide de l'information. Traditionnellement, le commandant interarmées exerce le commandement et le contrôle sur les forces présentes dans sa zone d'action, mais en MDO ce ne sera pas le cas pour les nouveaux domaines, cyber ou espace qui resteront dans la main des nations. Il faudra donc réfléchir en termes d'effets à produire plutôt que de capacités à avoir sous son contrôle.

L'adoption du *Digital Backbone*, dont la raison d'être est précisément de s'affranchir des obstacles potentiels pour livrer l'information au plus vite à celui qui en a besoin, aura nécessairement un impact sur la façon de déléguer l'autorité, sur la confiance du chef dans le système qui sera approvisionné par l'intelligence artificielle, sur le degré d'intervention humaine dans le processus, sans oublier les aspects moraux et légaux. Le centre d'excellence OTAN pour le commandement et le contrôle (C2CoE) a conduit une étude sur la physionomie du poste de commandement futur. Celui-ci serait à la fois géographiquement dispersé, pour éviter de regrouper les personnels sur un seul lieu, mais connecté en permanence par des flux sécurisés. Le personnel d'état-major serait renforcé par des assistants virtuels faisant appel à l'intelligence artificielle, chargés d'établir l'appréciation de situation et de proposer des modes d'action. Il s'agira donc de réorganiser les tâches, confier les tâches routinières à l'IA et à des algorithmes pour permettre à l'humain de se focaliser sur l'interprétation et la décision par rapport aux masses de données fournies.

Conclusion

La guerre en Ukraine fait certes appel à de nouvelles technologies comme les drones, ou le cyber, et utilise des plateformes « civiles » comme le téléphone portable pour localiser des cibles. Mais dans l'ensemble, elle reste encore un affrontement du passé, où tranchées, embuscades, chars d'assaut, artillerie restent largement les moyens ou les modes d'action les plus utilisés. Un conflit futur entre l'OTAN et un adversaire disposant des capacités équivalentes à celle de l'Alliance prendra très probablement une autre tournure.

La partie cinétique demeurera essentielle, mais elle ne pourra toutefois jouer son rôle que si elle s'intègre parfaitement dans un concept multidomaines, dont elle ne sera qu'une des composantes, celle chargée d'obtenir un effet dans la dimension physique. Il s'agira d'ailleurs de déterminer si c'est bien dans cette dimension qu'on veut obtenir un effet ou s'il vaut mieux le produire dans la dimension virtuelle ou cognitive. Tout le défi, au-delà de l'acquisition et de la mise en œuvre d'un système numérique fiable, rapide et sécurisé, sera d'éduquer et d'entrainer les opérateurs comme les commandeurs à savoir quels effets demander et à connaître les possibilités de ces moyens dont ils ne disposeront pas de manière organique.

Pour l'OTAN, il est urgent de se doter de ce *Digital Backbone* et de revoir sa structure de commandement qui s'appuie toujours, peu ou prou, sur le modèle de la Guerre froide, avec une hiérarchie d'états-majors statiques et volumineux, incapables de se disperser et de fonctionner en réseau comme l'exige le concept MDO. Les deux commandements stratégiques vont s'employer à revoir la copie, mais les lourdeurs administratives comme culturelles vont représenter le véritable défi du passage aux opérations multidomaines.

Crédit photo: OTAN

•— ••— — • ••— •—• •••

Olivier Rittimann

Général (2s) Olivier Rittimann. Après ses années de temps de troupe au sein de la Légion étrangère, le général de corps d'armée Rittimann a eu une seconde partie de carrière marquée par l'international, principalement dans des fonctions et à des postes au sein de l'OTAN (à Paris, Heidelberg, Bruxelles, Brunssum et Mons). Il a occupé en particulier le poste de représentant militaire français au SHAPE (*Supreme Headquarters Allied Powers Europe*, grand quartier général des puissances alliées en Europe), de chef d'état-major du commandement interallié de Brunssum et de vice-chef d'état-major du SHAPE. Il a commandé le collège de défense de l'OTAN, à Rome, de 2020 à 2023 et fait à présent partie de l'équipe des *Senior Mentors* au profit des exercices de l'OTAN.

Comment citer cette publication

Olivier Rittimann, « L'OTAN et les opérations multidomaines », *Le Rubicon*, vol. 3, 31 août 2023 [https://lerubicon.org/lotan-et-les-operations-multidomaines/].