UNIVERSITÉ PARIS 1 – PANTHÉON - SORBONNE –
Chaire Grands enjeux stratégiques contemporains

Connaissance et anticipation au cœur de la supériorité stratégique moderne

Hervé Multon | Directeur général adjoint, Stratégie, Recherche et Technologie, Thales.

Au regard des difficultés rencontrées ces dernières années pour l'emporter sur les théâtres d'opérations, on se dit qu'une réflexion sur les conditions de la supériorité stratégique doit être abordée avec modestie face à un sujet multidimensionnel et une réalité qui nous a mis à dure école. Partons donc d'un constat très simple qui ralliera les suffrages : malgré l'adage selon lequel Dieu est du côté des gros bataillons, la possession d'une supériorité écrasante dans les domaines technologiques, humains ou financiers ne garantit pas aujourd'hui la victoire ou le succès, tout au moins dans la durée. Connaître le milieu, comprendre l'opposant, anticiper ses activités sont devenus des nécessités face à la capacité de surprise et d'initiative d'adversaires qui, comme la guerre elle-même selon Clausewitz, sont des caméléons : changeants, fluides, réactifs, difficiles à distinguer des populations.

Prenant acte de ce défi, dès 2008, le *Livre blanc sur la défense et la sécurité nationale* a érigé le besoin de « connaissance et anticipation » en fonction stratégique. Il se trouve que la base technologique sur laquelle reposent les systèmes opérationnels propres à l'accomplissement de cette fonction connaît aujourd'hui des mutations sans précédent. Vont-elles changer la donne et procurer l'ascendant recherché ? Sans doute, à condition de bien comprendre et maîtriser les nouveaux risques liés au paradigme de l'information infinie et de replacer dans la chaîne technico-opérationnelle le facteur humain à sa juste place : la première.

De l'empire du capteur au règne des « *data* »

Ce qui caractérise sans doute le domaine du renseignement et de la surveillance-reconnaissance ces dernières années, c'est bien l'explosion du nombre de capteurs. Si naguère la préoccupation principale consistait à augmenter au maximum leurs performances – radar à plus longue portée, satellites d'observation à la résolution plus fine, largeur de bande des moyens d'écoute, précision des goniomètres… – aujourd'hui l'enjeu principal consiste plutôt à assurer la gestion et l'interconnexion entre tous ces capteurs.

Les moyens de collecte de l'information ont littéralement changé d'échelle : les drones peuvent se compter par centaines dans certains théâtres

(les États-Unis en possèdent plus de 7 500 à eux seuls), les satellites d'observation sont conçus en constellations ou réseaux pour assurer une surveillance accrue de zones toujours plus importantes, les sondes de cybersurveillance se multiplient sur les réseaux et systèmes d'information, les caméras urbaines se comptent par dizaines de millions… Parallèlement les capacités de stockage explosent (*cloud computing*), de même que les capacités de traitement et l'aptitude à la mobilité connectée large bande (*LTE 4G*). Si la loi de Moore décrite en 1971 reste très populaire avec l'annonce du doublement du nombre de transistors tous les dix-huit mois, il ne faut pas ignorer les progrès phénoménaux réalisés dans la miniaturisation : à performance égale, un satellite de renseignement de type *Helios* péserait aujourd'hui dix fois moins qu'il y a vingt ans. Nous attendons également beaucoup des nanotechnologies avec l'essor des microsatellites et l'émergence de nano-drones.

La multiplication de ces capteurs aboutit à un véritable changement de paradigme : l'information autrefois rare est devenue surabondante. La révolution stratégique induite par ce nouvel environnement peut être comparée aux bouleversements apportés par l'entrée dans l'ère nucléaire dans les années 1950. Si l'on avait à l'époque atteint une sorte d'infini dans les capacités de destruction, on s'affranchit aujourd'hui de toute limite dans l'information disponible et surtout dans la ressource numérique, au risque d'ailleurs de se retrouver sous un déluge de données.

L'enjeu n'est donc plus – seulement – l'acquisition de la donnée (la *data*) mais son traitement. Il s'agit d'être capable d'exploiter à notre profit, de transformer l'ensemble de ces données brutes en information intelligible, pour en extraire des éléments de connaissance, afin d'être en état d'anticiper et d'agir sur le cours des choses. La « préparation informationnelle » doit permettre de braquer un « télescope » sur une zone d'intérêt pour « tout savoir » en un minimum de temps quand il s'agit de décider et pour être prêt quand il faut intervenir : c'est la version moderne de la lunette de Napoléon ! Mais pour que cette capacité soit performante, cela nécessite de maîtriser la chaîne complète de la connaissance numérique – réseaux haut débit sécurisés terrestres et spatiaux, systèmes d'information, *cloud computing* privés, etc. – qui relie un ensemble de systèmes complexes, cohérents et interopérables afin de réduire le temps de décision et de l'action. Lors de l'opération *Harmattan*, par exemple, le temps entre la détection d'une cible par un capteur (imageur sur drone, pod de reconnaissance sur avion, satellite…) et son « traitement » en vue d'une frappe a été réduit à quelques minutes, l'étape la plus longue dans cette boucle de décision étant bien souvent la prise de décision humaine…

Enfin, on parera de mieux en mieux au risque de noyade dans l'océan de l'information grâce à l'émergence de technologies prédictives. Les algorithmes de *Big Data* peuvent désormais détecter des « anomalies » dans des millions de comportements humains, trahissant potentiellement une intention malveillante (foule dans un stade ou un métro, passagers dans un aéroport…).

On le voit bien, l'innovation de ces dernières années a profondément révolutionné cette capacité de « connaissance et anticipation » en lui apportant une profondeur inégalée. Néanmoins, cela ne se fait pas sans nouveaux risques qu'il serait dangereux d'ignorer.

De nouveaux risques liés à l'utilisation massive des nouvelles technologies

Tout d'abord, la diffusion massive des nouvelles technologies, il ne faut pas l'oublier, profite également aux adversaires potentiels. Des outils tels que *Google Earth* permettent désormais à tout le monde d'accéder à des images aériennes et spatiales du monde entier, et des prises de vue spatiale à haute résolution s'achètent dans le commerce. L'utilisation des réseaux sociaux a considérablement accru les capacités de renseignement humain d'individus ou d'organisations étatiques ou non étatiques.

En quelques années, le différentiel entre les moyens déployés par les armées les plus avancées technologiquement et ceux de leurs adversaires s'est significativement érodé. Dans certains cas, tel adversaire mafieux risque même d'être mieux équipé que les forces de sécurité chargées de le combattre.

Autre zone de risque croissante : la vulnérabilité des hautes technologies. Des adversaires, même rustiques, peuvent désormais très facilement accéder à des capacités de guerre électronique comme le brouillage de signaux *GPS* par exemple. D'autres plus évolués n'hésitent pas à s'en prendre aux réseaux de communication *via* le développement de cyberattaques.

Face à cela, les approches traditionnelles de cybersécurité – défense « périmétrique » des réseaux par « pare-feu », antivirus… – ne sont plus suffisantes. Il convient de développer une véritable politique de cyberdéfense autour du triptyque *renseignement*, *défense proactive des systèmes* (y compris ceux fonctionnant en continu comme les systèmes industriels), *capacités de riposte*. Cela repose sur le développement de nouvelles pratiques (surveillance des flux de données, tests d'intrusion…) et de nouvelles notions (sécurité native ou structurelle *by design*, architecture spécifique…).

L'équation gagnante : supériorité stratégique = (maîtrise technologique) x (facteur humain)

Selon l'expression du général Pierre Gallois, la stratégie du début de la Première Guerre mondiale consistait dans une large mesure à pouvoir aligner le maximum de poitrines mais l'enlisement des opérations montra vite la limite de l'approche. Aujourd'hui de manière analogue, il ne suffira pas d'aligner les capteurs et les ordinateurs pour prendre le dessus dans une crise ou un conflit. L'intelligence stratégique doit savoir utiliser ces ressources selon une logique dynamique face à un adversaire qui refuse nos règles du jeu, nous entraîne sur

des terrains peu favorables (villes ou montagnes), et crée la surprise par ses initiatives. Nos systèmes techniques complexes doivent alors être maniés par des systèmes d'hommes que caractériseront la qualité du jugement, l'aptitude au travail collectif obtenu par l'expérience et l'entraînement, et pour les meilleurs d'entre eux le fameux « coup d'œil » clausewitzien. En France, il me semble que le CPCO, le Centre de planification et de conduite des opérations à l'EMA, donne une belle image de cette réalité humaine : quelques hommes qui se connaissent par cœur qui sont habitués à travailler en symbiose parfaite, dont l'efficacité dans la conduite opérationnelle des interventions et la capacité d'interfaçage avec les échelons supérieurs de décision, est largement reconnue hors de nos frontières. « Un petit groupe d'hommes habitués à travailler ensemble », ainsi un très grand chef d'entreprise américain avait-il défini le secret du succès de sa société.

Prendre en compte le facteur humain : c'est aussi nécessaire dans l'intelligence de l'Autre. L'Altérité nous semble aujourd'hui une catégorie stratégique à part entière dans les conflits. Une mauvaise compréhension de l'adversaire, non seulement d'un *leader* ou du fonctionnement d'une équipe dirigeante, mais d'un pays et d'une société entière, peut stériliser ou contrecarrer l'efficacité dans l'emploi de la force militaire. L'altérité stratégique nécessite également de savoir renoncer à transformer le rival ou l'adversaire en « clone » de nous-mêmes : il n'appliquera pas les mêmes recettes tactiques ou techniques, à la fois par souci dialectique et parce qu'il part généralement d'une base culturelle différente C'est pourquoi la maîtrise des milieux physiques, généralement acquise dans la 3e dimension, disputée au sol dans les espaces cloisonnés, doit aussi s'accompagner de la maîtrise du « terrain humain ». Aux États-Unis, cela a donné lieu à de véritables programmes de formation des forces et de leurs chefs impliquant une grande variété de sciences humaines et sociales (sociologie, anthropologie, linguistique, connaissance des cultures régionales…). Le Commandement de la doctrine de l'Armée de terre a joué un rôle pilote à cet égard, bénéficiant d'une tradition américaine de coopération de l'Université à la mise au point des solutions de défense qui remonte à la Seconde Guerre mondiale.

C'est donc la conjonction de cette compréhension humaine et des nouvelles technologies qui peut faire la différence, un peu comme une arme qui ne donne son plein rendement que lorsqu'elle a trouvé le bon contexte d'emploi. Prenons l'exemple des *Big Data*. La plate-forme *Osintlab*, développée chez Thales, analyse les opinions et reconstruit automatiquement les réseaux cachés à partir de masses d'information gigantesques issues notamment du monde ouvert (*Web 2.0* : *blogs*, forums, réseaux sociaux, etc.). Elle aide puissamment l'analyste sans dispenser de l'expérience, de la culture et de l'« empathie ». Les technologies peuvent aider à trouver l'aiguille dans la botte de foin ; à condition de savoir que l'on recherche une aiguille !

C'est la qualité du groupe humain qui permettra de tirer parti de la technologie. Revenons donc à cette notion de systèmes d'hommes. Compétence,

expérience, formation sont naturellement des prérequis au plan individuel mais qui demeureront stériles sans l'interopérabilité humaine. Dans un groupe comme Thales, et sans doute dans les grandes organisations internationales publiques comme l'Otan ou l'Union européenne, l'aptitude au travail coopératif en environnement multiculturel est vue comme une compétence fondamentale.

L'interopérabilité humaine et culturelle favorise en effet la fertilisation croisée des technologies (Thales possède un portefeuille de plus de 12 000 brevets) au sein d'un groupe dont le spectre d'activités, du spatial aux transports en passant par l'avionique, les C4I de défense et de sécurité, les systèmes militaires embarqués, les opérations aériennes, est d'une grande variété. Elle contribue à éviter des cloisonnements qui finiraient par devenir fatals à la créativité et à la réactivité face aux évolutions des besoins et des marchés. Dans le domaine des radiocommunications militaires, par exemple, c'est l'union des compétences françaises et américaines qui procure l'avantage dans les technologies d'avenir comme la radio logicielle. Mais la fertilisation croisée ne peut se pratiquer en autarcie : il faut avoir aussi appris à travailler vers l'extérieur avec des laboratoires et des universités dont les cultures de travail, la sociologie propre (paramètres de carrière et d'avancement, critères de succès, conception de la hiérarchie), les cycles sont différents. C'est ainsi que les algorithmes de *Big Data* sont développés avec une université parisienne pionnière dans les mathématiques mondiales. Dans des contextes différents bien entendu, l'interopérabilité culturelle et humaine s'applique à la coopération avec des centaines de PME, indispensables sous-traitants ou partenaires de l'innovation technologique.

En vérité, le croisement des cultures est même sans doute aujourd'hui la condition *sine qua non* de la créativité. Quand le général Petraeus est arrivé en Irak, il a su modifier le cours des choses et endiguer le chaos civil et militaire grâce à une nouvelle doctrine de contre-insurrection, le *FM 3.24*, largement inspirée des travaux du Français Galula, qui avait écrit au moment de la guerre d'Algérie, et des conseils d'un officier australien. D'une manière générale, comme l'ont montré certains historiens et anthropologues, l'innovation est rarement endogène et n'est souvent qu'une bonne pratique ou une idée banale empruntées à un domaine différent de celui dans lequel on opère.

⁂

Connaissance, anticipation, jugement et créativité : après examen, c'est donc le quadriptyque que l'on a envie de proposer pour résumer notre approche de la supériorité stratégique et militaire au XXIe siècle. L'aptitude au jugement, privilège que l'humain conservera toujours face à l'ordinateur, prend d'autant plus de valeur que la technique, selon la formule de Martin Van Creveld, peut inciter à croire que la réalité est prédictive et linéaire, quand l'expérience et l'histoire ne cessent de mettre en scène les ruptures et la non linéarité. À cet égard, la créativité pour répondre au non linéaire dépendra aussi du système d'hommes que l'on aura construit en croisant efficacement expériences et cultures.