

Les enjeux et la numérisation du renseignement futur

Développer les capacités de renseignement de l'Etat et plus particulièrement des forces armées est un vœu exprimé régulièrement par nos responsables politiques et militaires. Mais au-delà du simple souhait, qui traduit un réel besoin, il semble utile de **se pencher sur les véritables enjeux du développement de nos capacités de renseignement** et de déterminer en quoi la numérisation des forces armées permettra peut-être de trouver des réponses aux défis ainsi posés.

La révolution dans les affaires militaires de la fin du 20^e siècle a donné lieu à **l'émergence de nombreux concepts novateurs**, voire porteurs de ruptures, dans le panorama stratégique et tactique, notamment des puissances occidentales.

D'une part la nature et les conditions des engagements militaires forcent et continueront sans doute à forcer les armées à l'acquisition de compétences multiples, plus seulement tournées vers l'action de guerre, face à des menaces très évolutives.

D'autre part, **la numérisation** qui représente, quoiqu'on en dise, **une véritable rupture technologique**, a propulsé les fonctions opérationnelles classiques vers une nouvelle ère.

La recherche permanente d'accroissement des facteurs "rapidité de l'action" et "atteinte à distance de l'adversaire", franchit un palier supplémentaire, dont les notions de connaissance de situation en temps (quasi) réel et de délivrance d'effets hors de la vue directe sont les principales traductions.

Dans ce cadre, le renseignement, au sens de la fonction, comme toutes les fonctions opérationnelles, **est en pleine transformation**. Pour ce qui la concerne, le concept novateur associé est nommé ISTAR par les Anglo-saxons, que nous traduisons par le terme SA2R (surveillance, acquisition, reconnaissance et renseignement) dont la concrétisation est un réel défi.

Partant du cadre des conditions des engagements actuels et futurs probables, dont tout particulièrement l'étude des menaces émergentes, il est ainsi possible de dégager les principaux enjeux pour le renseignement futur et d'identifier en quoi la numérisation, là encore, sera porteuse de ruptures tactiques et techniques pour tendre vers la nécessaire concrétisation du concept SA2R.

PAR LE COLONEL BERTAND CHANDOUINEAU, DU BUREAU CONCEPTION DES SYSTÈMES DE FORCES DE L'EMAT

Les menaces émergentes peuvent être catégorisées selon leurs caractéristiques majeures

Les **menaces dites symétriques ou dissymétriques** reposent sur **trois principes** :

- La **réalisation de modes d'actions plutôt conventionnels**, qui respectent

généralement les principes de guerre et ses règles. Même dans le cas d'un affrontement du faible au fort, l'engagement reste militaire, il est le plus souvent frontal au moment du contact et la tactique militaire guide l'action.

- L'**emploi de systèmes d'armes généralement similaires aux nôtres**, qui

provoquent des situations de duel relativement équilibrées. Un char, un avion de combat ou un fantassin, même moins performants, entrent dans des catégories identifiées et restent des systèmes qui peuvent rivaliser avec les nôtres.

- Les **organisations et les procédés tactiques** nous sont relativement connus. En effet,

peu d'armées "organisées" sont aujourd'hui ignorées des services de renseignements en général, ce qui confère à chacun une connaissance a priori de l'adversaire, qui peut être désigné.

Nos forces armées bénéficient d'emblée, face à ces menaces dites symétriques ou dissymétriques, d'avantages opérationnels. Le rapport de forces

reste classique et peut être mesuré, la réponse à apporter au danger que représentent ces menaces est la plupart du temps connue et applicable et, surtout, **la nature exacte des menaces peut être cernée, ce qui permet l'anticipation et le déroulement des modes d'action traditionnels de la fonction renseignement.**

En revanche, **les menaces de nature asymétrique** posent à la fonction renseignement de vrais défis à relever, car elles reposent sur **trois principes plus complexes** que les principes précédents :

- **La terreur comme moyen d'atteindre l'objectif général.** Celle-ci s'obtient par des modes d'action la plupart du temps non conventionnels, sans respect des règles de la guerre et son impact psychologique est très fort. Ainsi, les cibles privilégiées sont les moins protégées naturellement (populations civiles) ou les plus vulnérables des forces militaires (réseaux de communication, systèmes logistiques, organisations de soutien en général, environnement humain de la force). Au plan tactique, ces menaces s'appuient sur la "foudroyance" de l'action, de même qu'au plan moral, elles reposent sur le fanatisme des combattants.

- **L'imprévisibilité de leur déclenchement** qui confère à ces menaces la possibilité de densifier le "brouillard de guerre". En effet, par leur présence permanente et l'implication des populations civiles au sein desquelles évoluent de plus en plus les forces, par l'influence des réseaux de tous types qui peuvent concourir à leur montée en puissance et grâce aux modes d'action originaux sans cesse renouvelés qu'elles emploient, ces

menaces présentent un véritable caractère d'ubiquité et peuvent demeurer surtout invisibles jusqu'à leur déclenchement.

- **La fluidité, enfin, des vecteurs de ces menaces**, qui est un principe qui lie leur furtivité à leur caractère insaisissable. En effet, le résultat tactique obtenu par une petite équipe peut avoir autant d'effet que celui obtenu par une unité militaire classique sans en avoir "l'empreinte", et l'affrontement en milieu ouvert est remplacé par l'affrontement en terrain urbain, complexe et masqué, où la population devient un abri. De plus, l'individu compte peu et des technologies très différenciées dont certaines modernes (la numérisation) et d'autres archaïques (le couteau qui permet d'exécuter l'otage) sont employées avec une aisance redoutable. Par leur fluidité, ces menaces "imprègnent" véritablement l'action militaire des forces armées classiques.

Face à ce dernier type de menaces, **qui permet à un adversaire, déclaré ou non, de posséder une part effective de supériorité opérationnelle sur les forces armées et de contrer efficacement les efforts du renseignement militaire classique**, il convient dès à présent de doter nos organisations de nouvelles capacités.

L'acquisition de nouvelles capacités

De nouvelles capacités doivent être acquises de manière à contrer le plus efficacement possible les menaces futures de tout type.

La première de ces capacités est **l'extension du champ de vision** des forces armées. Celle-ci sera d'abord permise par un changement culturel profond qui mettra dans l'esprit de chacun, en particulier des chefs interarmes et interarmées et surtout de chaque intervenant opérationnel des forces, le "sens" du renseignement, des échelons de commandement les plus

élevés aux échelons tactiques. Au-delà, une multiplication des capteurs et l'appel à des technologies adaptées aux conditions modernes d'engagement (zone urbaine, aide technique aux capteurs humains, capacités tout temps,...) seront nécessaires.

La capacité suivante à acquérir concerne **le suivi des vecteurs de menaces**. Celui-ci permettra de ne pas perdre de vue des menaces montant en puissance quand elles auront été détectées, de manière à diminuer leur furtivité. Outre la multiplication des capteurs et l'appel à des technologies adaptées, cette capacité reposera sur une accélération de l'exploitation des informations et une meilleure coopération entre "services", mais aussi, en interne des forces, entre les armées et entre les armes.

Enfin, la capacité de **connaissance des adversaires**, déjà présente, devra être amplifiée par une augmentation de la capacité d'exploitation du renseignement et une meilleure organisation de sa capitalisation.



SIRPA TERRE

La combinaison de ces trois capacités permettra l'acquisition de la capacité globale que représente la **compréhension des menaces et de l'environnement**, nécessaire demain à l'anticipation dont les forces armées devront faire de plus en plus preuve. C'est bien cette dernière capacité qui doit fonder l'ensemble de la réflexion en matière de renseignement futur, dont la numérisation est un des facteurs constitutifs déterminants.

La numérisation des forces armées permet de répondre à chacune des nécessités d'évolution décrites précédemment

Cette numérisation peut permettre le passage du renseignement classique au concept SA2R (surveillance, acquisition, reconnaissance et renseignement). Une définition courte de ce concept pourrait d'ailleurs être la suivante :

“Permis par la numérisation, le concept SA2R vise à offrir la perception **permanente** la plus **précise, complète, juste, pertinente** et **actualisée** de la situation des *adversaires*, des *menaces* et de l'*environnement* par la **féderation de l'ensemble des informa-**

tions utilement partagées selon le temps et le besoin d'en connaître”.

C'est bien la **numérisation** qui permettra ainsi de développer les capacités nouvelles précitées, en particulier par le développement de **plusieurs principes**.

Il deviendra nécessaire en premier lieu de (re)donner une **dimension réellement tactique** à l'obtention du renseignement, en considérant que, chaque soldat étant un capteur en puissance, l'information qu'il obtient doit être utilement diffusée, lui permettant de participer ainsi à l'élaboration du renseignement global.

La numérisation permettra d'envisager également une **multiplication du nombre de capteurs**, sans forcément multiplier le nombre de plateformes dédiées à cette fonction, mais en intégrant par exemple des technologies complémentaires sur les mêmes vecteurs. Une partie de ces vecteurs devra être robotisée, de manière à éviter les pertes humaines et à assurer une réelle permanence. Les drones représentent déjà la concrétisation de tels vecteurs multi-capteurs et robotisés. Les capteurs devront de plus être liés entre eux, de manière à en accroître la synergie, mais être

également liés aux producteurs d'effets pour accroître la rapidité d'action et l'efficacité de ces derniers. Par ailleurs, des **technologies spécifiquement adaptées** aux besoins devront être développées, dont en particulier des technologies d'imagerie, radars et électromagnétiques de détection de nouveaux signaux.

Au-delà, l'indispensable accélération de l'exploitation du renseignement sera rendue possible en particulier par la **fusion**, qui peut être définie comme la double capacité automatisée d'aide à la corrélation de données et d'aide à l'agrégation de situations. C'est la fusion qui autorisera une validation quasi instantanée du renseignement et permettra ainsi de suivre effectivement les vecteurs de menaces. Elle figure donc **au cœur des capacités futures de renseignement**.

De plus, l'accroissement de la coopération entre “services” afin d'élargir ainsi le champ du renseignement d'intérêt militaire correspondra rapidement à une impérieuse nécessité. La numérisation permettra justement plus aisément cette coopération au travers notamment d'une meilleure organisation de la **capitalisation du renseignement** et du **lien entre des bases de données struc-**

turées en vue d'une exploitation partagée, rapide et rationnelle. Enfin, le développement **d'outils numériques spécifiques** tels qu'on en trouve déjà les prémices, en particulier en intelligence économique, et dont l'armée de terre souhaite se doter au travers du projet **SORA** (système d'optimisation du renseignement aéroterrestre) permettra d'augmenter la capacité d'exploitation et la puissance d'analyse.

Cette évolution vers la concrétisation du concept SA2R et le développement des capacités décrites aura bien entendu des conséquences directes, en particulier sur la fonction renseignement, tant en matière de ressources humaines (nouveaux métiers et volumes d'analystes), de formation et d'entraînement (formation des acteurs du renseignement, entraînement multicapteurs, simulation du renseignement), d'équipements (nouveaux systèmes de capteurs, d'information et de communication) et d'organisation (unités multi-capteurs).

Ces conséquences semblent lourdes à assumer à l'heure où les budgets et les effectifs des armées sont comptés. Mais, sauf à admettre un aveuglement et une surdité grandissantes face aux menaces qui ne manqueront pas d'être omniprésentes autour des engagements militaires, il semble également qu'il faille **accepter d'en payer le prix et de marquer un véritable effort sur la numérisation de la fonction renseignement**.