Le renseignement militaire français a au moins trois défis à relever

Posté dans [Renseignement](http://www.opex360.com/category/renseignement/) par [Laurent Lagneau](http://www.opex360.com/author/admin/%22%20%5Co%20%22Articles%20par%20Laurent%20Lagneau) Le 26-12-2018



**La Loi de programmation militaire [LPM] 2019-25, comme les deux précédentes, fait du renseignement une priorité**.

**Ce qui passera par le renouvellement des moyens spatiaux** [programmes MUSIS qui renforcera les capacités d’observation optique et radar et CERES, pour l’écoute et le renseignement électromagnétique], la mise en service de drones MALE supplémentaires, d’avions légers de surveillance et de reconnaissance, de la charge utile de guerre électronique [CUGE] ainsi que par la commande d’un bâtiment léger de surveillance et de recueil de renseignement [BLSR], qui viendra compléter le Dupuy de Lôme.

Au total, 4,6 milliards d’euros d’investissement sont prévus, auxquels on peut ajouter 1,6 milliard consacrés au cyberespace.

Le renforcement de ces capacités supposera donc un flux toujours plus important de données et d’informations à analyser.

Aussi, pour la Direction du renseignement militaire [DRM], l’un des enjeux sera de [recruter](http://www.opex360.com/2018/03/31/direction-renseignement-militaire-peine-a-recruter-sein-armees/) suffisamment d’analystes.

Et surtout de les garder, sachant que des spécialités sont actuellement déjà déficitaires et qu’il faut par exemple deux ans pour former un linguiste militaire…

Mais plus généralement, la « massification » des données est l’un des défis qu’a à relever la DRM. C’est en effet ce que son directeur, le général [air] Jean-François Ferlet, a avancé dans le [dernier hors-série du magazine DSI](https://www.areion24.news/produit/dsi-hs-n-63/), dédié au renseignement militaire.

« La masse des données numériques et la gestion de la connaissance, qui, au-delà du big data ou de l’IA [intelligence artificielle, ndlr], obligent à disposer d’une capacité ad hoc d’exploitation des données », a expliqué le général Ferlet**.**

**« La masse des données issue des investigations dans le cyberespace, de capteurs hautement performants, de capacités nouvelles comme la biométrie, des échanges avec les partenaires, ou encore la veille stratégique élargie, pose l’enjeu crucial de leur exploitation et de la construction de la connaissance qui reposera sur le croisement efficace de ces données hétérogènes », a-t-il insisté.**

**Pour cela, le général Ferlet mise évidemment sur la numérisation, le big data et l’intelligence artificielle, ces technologies devant permettre d’automatiser certaines tâches**.

 Cependant, ces dernières ne doivent pas être une fin en soi. « L’analyste doit pouvoir garder son autonomie et ne pas s’en remettre uniquement aux outils, aussi innovants soient-ils. Dans le processus analytique [au sein de la DRM], l’usage de l’AI doit donc être raisonné », a-t-il expliqué.

Toutefois, ces outils, pourvu donc que l’on en fasse un usage raisonnable, sont plus que jamais nécessaires au regard des deux autres défis de la DRM.

**L’un porte sur « le traitement d’une menace accrue sur tout le spectre, à la fois globale, locale et fragmentée, matérielle et immatérielle, liée à des États ou des groupes d’individus isolés** », a indiqué le général Ferlet.

 Or, a-t-il ajouté, cette « menace se rapproche du territoire national » et la « DRM doit appuyer toujours plus efficacement les armée sur les théâtres ouverts, tout en veillant sur le reste du spectre pour garantir l’autonomie d’appréciation des autorités militaires et politiques, éclairer les choix capacitaires et anticiper les déploiements futurs ».

En outre, et c’est là un autre défi pour la DRM, de nouveaux « fronts » porteurs de menaces apparaissent, dont, a détaillé le général Ferlet, **« l’espace exoatmosphérique, le cyberespace, les armes à effets dirigés et nucléaire, radiologique, bactériologique et chimique. »**

 Selon lui, ces « nouveaux domaines de conflictualité appellent à investir de nouvelles compétences et à appréhender le RIM [renseignement d’intérêt militaire] qui s’y greffe ». En un mot, cela demande le recrutement (ou la formation) de nouveaux spécialistes.

Pour relever ces défis, le général Ferlet espère que la DRM aura achevé sa transformation numérique d’ici 2030. « Par ses capacités augmentées, elle sera pleinement investie dans les nouveaux espaces, cyber et spatial », avec une « ressource humaine à dominante militaire multifonction et formée à la statistique et au data mining ». Le tout en se reposant sur un « écosystème stimulant d’entreprises françaises consacré à l’innovation au profit du renseignement », via le pôle de compétitivité « Intelligence Campus », à Creil.