ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

Jeudi
8 mars 2018
Séance de 9 heures

Compte rendu n° 52

SESSION ORDINAIRE DE **2017-2018**

Présidence de M. Jean-Jacques Bridey, *président*

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures.

M. le président Jean-Jacques Bridey. C’est la première fois, Mon général, que nous vous recevons pour une audition. De nombreuses questions vous seront donc certainement posées. De votre côté, je ne doute pas que vous ayez beaucoup de choses à nous expliquer relativement au fonctionnement de votre direction, comme au sujet du contenu du projet de loi de programmation militaire (LPM).

M. le général Jean-François Ferlet, directeur du renseignement militaire. Merci Monsieur le président pour votre accueil. Je vous exposerai quels sont, vus de la direction du renseignement militaire (DRM), les enjeux de cette LPM.

Permettez-moi tout d’abord de me présenter. J’ai débuté ma carrière dans l’armée de l’air comme pilote de chasse, spécialisé dans un premier temps dans la défense aérienne, puis dans un second temps dans la reconnaissance aérienne tactique. Assez classiquement, ma carrière m’a mené du commandement d’un escadron de reconnaissance à celui de la base aérienne de Djibouti. Ces engagements ont été entrecoupés de passages en état-major dans le domaine des plans et des programmes d’armement liés à la fonction renseignement.

En deuxième partie de carrière, mes engagements ont été avant tout opérationnels : en 2014-2015, j’ai ainsi effectué une année dans le Sahel, en tant que général adjoint chargé des opérations de l’opération Serval, pour le premier mois, puis de l’opération Barkhane, pour les onze mois suivants. À l’issue, j’ai pris le commandement du centre de planification et de conduite des opérations, qui est l’outil de commandement stratégique de toutes les opérations militaires françaises, tant sur le territoire national qu’à l’étranger. Il est situé à Balard. Mon tropisme est donc plutôt opérationnel. Cela me permet de ne pas perdre de vue l’une des raisons d’être de la DRM.

Le projet de LPM fait clairement porter l’effort sur la fonction de connaissance et d’anticipation, qui comprend à la fois nos capacités dans le domaine du renseignement et celles du monde cyber. Il répond ainsi à de nombreuses attentes de la DRM, notamment en matière de ressources humaines, de finances, de grands programmes d’armement et de dispositions normatives.

Avant d’entrer dans le vif du sujet, je vous brosserai un rapide tableau de la DRM dans son environnement. Pour rester simple, la direction du renseignement militaire est le service de renseignement des armées. Je remplis ma mission sous une double tutelle, puisque je sers sous les ordres du chef d’état-major des armées, mais je suis également conseiller de la ministre des Armées en matière de renseignement d’intérêt militaire.

Au niveau interministériel, je fais partie des six directeurs des services de renseignement, dit du « premier cercle », regroupés autour du coordinateur national du renseignement et de la lutte contre le terrorisme. Au niveau international, j’entretiens d’importants échanges avec mes homologues étrangers des services de renseignement partenaires.

Ma mission se résume en trois volets. Le premier aspect a trait à l’appui direct en renseignement aux opérations. La DRM déploie des hommes et des capteurs sur les théâtres d’opérations et participe activement à l’analyse du renseignement collecté sur ces zones.

Vient ensuite l'anticipation, conçue comme une aide à la prise de décision et à la réorientation des actions ; dans ce domaine, nous travaillons à un horizon de six mois à un an. Enfin, la veille stratégique est une mission permanente, que nous remplissons au quotidien en complément de ces deux premières missions.

La DRM est en interaction avec de nombreux acteurs ; elle appartient concurremment à trois ensembles.

Le premier constitue la famille interarmées du renseignement ; la DRM y travaille en étroite collaboration et concertation avec les armées. La DRM compte un peu moins de 2 000 personnes, tandis que la fonction interarmées du renseignement (FIR), c'est-à-dire les capacités de renseignement mises en œuvre par les armées, représente environ 8 000 personnes supplémentaires, qui disposent de moyens dédiés, variant selon leur milieu d'exercice.

Au sein de cette FIR, j'occupe la fonction de « tête de chaîne ». Sur des sujets aussi divers que le domaine capacitaire, la formation, le recrutement, le pilotage des métiers du renseignement, la doctrine et la coordination des programmes majeurs, la DRM joue un rôle de coordination. Je veille ainsi à ce que toutes les actions lancées dans le domaine du renseignement soient les plus cohérentes possible.

Le deuxième ensemble constitue la communauté nationale du renseignement. S'y trouvent les six services de renseignement du « premier cercle » : direction générale de la sécurité extérieure (DGSE), direction générale de la sécurité intérieure (DGSI), le service du traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN), la direction nationale du renseignement et des enquêtes douanières (DNRED) et la direction du renseignement et de la sécurité de la défense (DRSD), regroupés avec la DRM autour de M. le préfet Pierre Bousquet de Florian, coordonnateur national du renseignement et de la lutte contre le terrorisme (CNR-LT).

Nous nous réunissons au moins tous les quinze jours pour traiter des sujets qui intéressent l'ensemble de la communauté nationale du renseignement, comme la formation de nos agents par l'Académie du renseignement, la mutualisation des capacités techniques des services de renseignement ou la coordination de nos partenariats internationaux. Au travers d'une structure de coordination rassemblant l'ensemble des services, l'état-major des armées (EMA) et la direction générale de l'armement (DGA), nous suivons les programmes qui ont fait l'objet d'une mutualisation, non seulement pour des raisons d'économie et de coût, mais aussi pour des raisons d'efficacité, de convergence et d'interopérabilité. Le dialogue est donc très fluide entre nos services.

Nous sommes le service référent dans le domaine de l'image et la DGSE l'est dans le domaine du renseignement d'origine électromagnétique. Élaboré sous l'égide du CNR-LT, le plan national d'orientation du renseignement (PNOR) fixe nos orientations. Il détermine, pour chaque service, qui est « menant » et qui est « concourant » sur tel ou tel sujet.

Le troisième ensemble constitue la communauté des services de renseignement au niveau international. La DRM échange des informations avec un peu plus de 70 pays dans des conditions très cadrées et normées. Nous étendons d'ailleurs encore ce réseau.

Le partenariat avec nos homologues étrangers s'inscrit à différents niveaux. Au premier rang de nos partenaires se trouvent bien sûr les Américains. Nous avons énormément d'échanges avec eux, au niveau central, entre agences de renseignement, et sur le terrain, notamment au Sahel où le soutien américain en moyens aériens de surveillance et de reconnaissance est déterminant pour nos opérations.

Ces échanges de renseignements avec les Américains sont très importants. Ils se sont encore développés davantage depuis l'été dernier, sous l'impulsion du Secrétaire à la Défense, le général James Mattis. Il souhaite en effet que les services de renseignement américains travaillent beaucoup plus avec leurs partenaires étrangers, notamment la France qui est un acteur volontaire, crédible et particulièrement engagé dans la lutte contre le terrorisme. Mais sans aller jusqu'à une formule de *Six Eyes*, nous avons obtenu des accords bilatéraux de partage du renseignement.

Nous avons d'autres partenaires, à différents niveaux. Notre premier partenaire, au niveau européen, est l'Allemagne. Nos relations et nos échanges sont marqués par un haut niveau de confiance. Cela nous permet d'aller très loin dans les échanges de renseignement, notamment dans le domaine de l'imagerie spatiale. L'Allemagne est aussi notre principal partenaire capacitaire, comme en témoigne sa participation déterminante au programme d'observation CSO (composante spatiale optique).

N'oublions pas d'autres échanges internationaux, qui ont lieu sous l'égide de l'Organisation du traité de l'Atlantique Nord (OTAN) ou de l'Europe de la défense. Dans le cadre de cette dernière, le président de la République a lancé en septembre dernier une nouvelle initiative, l'Initiative européenne d'Intervention (IEI), visant à développer une culture stratégique et opérationnelle commune entre pays désireux de mettre en place une capacité européenne d'intervention renforcée. Un de ses volets consistera à former un équivalent du groupe d'anticipation stratégique (GAS) français, permettant de partager une vision des grands enjeux à un horizon de deux ans – car il ne sert à rien de travailler au-delà de cet horizon dans ce cadre. Nous voulons également œuvrer ensemble sur des sujets d'intérêt commun. Les États approchés pour participer à cette initiative devraient signer fin mai une lettre d'intention qui définira la manière dont nous allons travailler de concert.

En matière de renseignement, l'Europe de la défense existe déjà d'une certaine manière. Nous avons en effet établi des partenariats de partage capacitaire dans le domaine spatial, ayant signé des protocoles de coopération avec certains pays européens. Ces coopérations fonctionnent bien. La France est à la pointe du renseignement en imagerie spatiale optique, alors que l'Allemagne s'est spécialisée dans l'imagerie spatiale radar. Le radar a l'avantage de fonctionner par tous les temps. Il est d'une autre nature que l'imagerie optique et apporte des renseignements très complémentaires.

Au sein de la communauté Helios ainsi constituée, nous partageons avec nos partenaires des images de nos satellites contre des images des satellites radar allemands SAR-Lupe mais aussi des images des satellites radars italiens COSMO-SkyMed.

S'agissant de l'OTAN, les choses sont un peu différentes. Évidemment, lorsque nous participons à une opération de l'OTAN, nous partageons notre renseignement avec l'Alliance et les pays alliés engagés. Nous sommes ainsi engagés dans le dispositif de l'OTAN « *Enhanced Forward Presence* » (EFP) déployé dans les pays baltes et qui contribue au

mécanisme de réassurance dans le cadre de la défense collective des pays de l'OTAN. Nous lui apportons un appui en matière de renseignement, en produisant quasiment quotidiennement des notes destinées aux pays de l'OTAN participant à ces opérations. Les productions de la DRM sont d'autant plus appréciées que rares sont les pays qui disposent, comme la France, d'une palette de capteurs large et complète, permettant de garantir une autonomie stratégique.

J'attire votre attention sur un point particulier. En matière de renseignement, la règle veut que les échanges reposent sur une logique de réciprocité. La seule exception à cette règle est notre soutien sans réserve et sans contrepartie à tous les pays européens qui s'engagent au Sahel, que ce soit dans le cadre de l'opération Barkhane, de l'EUTM ou de la MINUSMA, mission de l'ONU de maintien de la paix au Mali.

Je conclurai sur la coopération en abordant le soutien que nous apportons à l'initiative des pays du G5 Sahel. Ils viennent de mettre sur pied la « force conjointe Sahel » et ont besoin d'un soutien en renseignements pour pouvoir agir efficacement. La France leur fournit ce soutien et nous leur apportons également un appui dans le domaine de la formation, du conseil, du *monitoring*, de façon à leur permettre de monter en puissance sur le volet renseignement.

J'en termine ainsi sur les principales missions et sur l'environnement de la DRM. J'en viens aux principaux défis auxquels elle est confrontée aujourd'hui.

Le premier défi est opérationnel. Un fort tropisme oriente nos capteurs vers la lutte antiterroriste. Elle constitue en effet une menace immédiate. Mais nous sommes aussi en charge de l'anticipation et de la veille stratégique, de sorte que nous veillons à garder un juste équilibre entre nos différentes missions. Les États-puissances font leur retour et de nouveaux acteurs proliférants apparaissent : nous devons garder un œil de ce côté, en continuant à suivre leur évolution, leur stratégie et leur montée en puissance. Nous nous devons en effet de nous prémunir contre toute surprise stratégique. Ce grand écart doit être tenu en permanence. La veille stratégique participe en effet de la crédibilité de notre dissuasion nucléaire.

Plus technique, le second défi est celui du *big data* et du traitement de masse des données. Nous devons faire porter notre effort sur ce domaine. Par le passé, nous nous sommes concentrés sur le renouvellement de nos capacités en matière de capteurs. Mais ce renouvellement des systèmes satellitaires est désormais acquis.

Le renseignement recueilli provient de quatre origines : les capteurs électromagnétiques, les images, le renseignement humain et le renseignement d'origine cyber, qui se développe très rapidement. Dans ce dernier cas, il s'agit de sources plus ou moins ouvertes.

Or, aujourd'hui, les capacités toujours plus grandes de ces capteurs, disposant d'un débit toujours plus élevé, nous placent en face d'un « tsunami des données ». Nous sommes submergés par des données dont la masse croît de manière exponentielle. Il ne saurait être question d'y faire face en se contentant seulement de demander des moyens supplémentaires en exploitants ou en analystes. Nous devons au contraire trouver des solutions plus innovantes, à base d'outils d'intelligence artificielle. Voilà où nous devons porter nos efforts dans les années qui viennent.

Il ne sert en effet à rien de collecter toujours plus de données et de renseignements si nous n'arrivons pas à les exploiter en tirant de nos bases des données les informations pertinentes au moment utile.

D'un point de vue technique, un deuxième défi se pose à nous. Chacun avait autrefois tendance à développer ses propres réseaux sécurisés, puisque nous traitons tous d'informations sensibles. Aujourd'hui, au contraire, le besoin accru d'échanger des renseignements, que ce soit d'un ministère à l'autre ou avec nos partenaires internationaux, nécessite des réseaux sécurisés et interconnectables. Cet impératif se révèle parfois difficile à concilier avec celui de la sécurité des opérations et de la protection de nos sources les plus sensibles. L'interconnexion et l'interopérabilité des réseaux constituent donc un autre défi.

Globalement, dans les domaines techniques, la technologie évolue très vite. Or ce n'est pas forcément la technologie militaire qui entraîne le mouvement. C'est pourquoi les programmes d'armement classiques, tels qu'ils sont menés sous l'égide de la DGA, ne sont pas forcément adaptés à l'évolution de ces nouveaux outils très évolutifs que sont les systèmes d'information. Puisque la technologie transforme rapidement les usages, nous constatons souvent qu'il existe des outils disponibles « sur étagère » déjà susceptibles, moyennant quelques adaptations, de répondre à nos besoins.

Sous l'égide de l'initiative « Innovation défense » portée par la DGA, avec l'appui attentif de la ministre des Armées et le soutien des armées, la DRM va développer l'*intelligence campus*. Il s'agit de regrouper autour de nos centres, pour l'essentiel basés à Creil, des capacités du monde académique, du monde de la recherche et du monde l'industrie. La mise en relation directe de ces différentes personnes et de ces compétences va nous permettre d'améliorer le cycle d'acquisition de ces nouveaux outils qui évoluent très vite dans le civil. Nous nous devons donc de nous adapter en permanence. L'initiative prochainement lancée s'appuiera ainsi sur le triptyque suivant : monde universitaire, recherche et acquisition.

Tous ces défis ne sauraient nous faire oublier les exigences fortes qui pèsent sur la DRM aujourd'hui.

Je commencerai par la conformité avec le cadre légal, qui est en évolution permanente. La loi du 24 juillet 2015 définit le renseignement comme une politique publique qui concourt à la stratégie de sécurité nationale et à la défense des intérêts fondamentaux de la Nation. Cette politique relève de la compétence exclusive de l'État. Cette loi a été complétée par celle du 30 novembre 2015 relative à la surveillance des communications internationales et par celle du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, qui comporte des dispositions relatives aux interceptions empruntant la voie hertzienne.

L'ensemble de ces dispositions ne s'applique qu'aux mesures mises en œuvre sur le territoire national ou à partir du territoire national. Compte tenu de ses missions en opérations en dehors des frontières, la DRM est donc moins « touchée » par la loi que les services qui agissent sur le territoire national. Néanmoins, la mise en œuvre de ces techniques de renseignement a nécessité une adaptation de nos outils.

Traditionnellement, nos linguistes, intercepteurs et analystes travaillaient directement « au pied du capteur » dans nos centres d'écoute. Aujourd'hui, pour permettre à la Commission nationale de contrôle des techniques de renseignement (CNCTR) de contrôler

effectivement nos activités, nous devons rapatrier les interceptions électromagnétiques dans des *data center*, que nous appelons des entrepôts, et en avoir une traçabilité complète.

Cela requiert une adaptation à ce cadre légal de nos outils, mais également de nos techniques de travail. L'exploitation en mode « centralisée » nécessite ainsi des supports particuliers. Certains outils développés dans le cadre de la mutualisation technique constituent la première brique d'un édifice d'exploitation des données qui sera fondé sur l'intelligence artificielle.

La seconde exigence qui pèse sur nous est de nous adapter en permanence à la menace, ou du moins à l'environnement et aux techniques utilisées par ceux qui nous intéressent. L'emploi des technologies numériques, typiquement les *smartphones,* se banalise, tout comme l'utilisation des réseaux sociaux. Certaines messageries très sécurisées, telles Whatsapp ou Telegram, nous posent de réelles difficultés.

Face à ce défi qui confère des capacités nivelantes à nos adversaires, l'enjeu est d'abord de réagir vite et moins de voir loin, même si ces deux enjeux ne sont pas nécessairement antagonistes.

Un premier frein existe dans ce domaine de l'innovation et du renseignement. Par exemple, il est difficile de donner à des acteurs privés l'accès à des bases de données contenant des informations sensibles. Jusqu'à présent, toutes les règles de sécurité ont été édictées dans une logique de recherche du risque zéro. Nous travaillons aujourd'hui pour évoluer vers une approche du risque maîtrisé.

Un autre frein culturel est la peur de l'échec. Quand le ministère lance un programme d'armement, beaucoup de précautions sont prises en amont, comme la conduite d'études de levée de risques. Ainsi, nous ne lançons un programme qu'en ayant minimisé le risque. Pourtant, les montants en jeu ne sont pas tous comparables à ceux des grands programmes d'armement. C'est un domaine où nous devrions accepter de prendre plus de risques, quitte à nous tromper parfois. Si nous faisons fausse route, nous devons pouvoir abandonner un outil et nous intéresser à un autre.

Aujourd'hui, notre « culture d'entreprise » est au contraire si prégnante que nous ne commençons un programme d'armement qu'en ayant la certitude de pouvoir le mener à terme. Compte tenu des coûts engagés, il serait cependant possible de prendre quelques risques dans le domaine de l'innovation, où des *start-up* offrent parfois des solutions méritant d'être explorées.

La troisième exigence qui pèse sur la DRM est l'amélioration permanente de la coopération et de la coordination entre les services, rappelée dans la Revue stratégique.

Nous sommes loin des clichés habituels de la « guerre des services ». Il existe une vraie collaboration entre les services, dont je peux témoigner. Au-delà des réunions destinées à traiter de sujets communs, qui se tiennent tous les quinze jours autour du CNR-LT, les services coopèrent entre eux au quotidien : au niveau central, en échangeant tous les documents qui pourraient intéresser les uns et les autres ; et à un niveau plus subsidiaire, lorsque nous avons des sujets d'intérêt commun, en créant des cellules *ad hoc*.

La plus importante est la cellule Allat, dédiée à la lutte antiterroriste et hébergée par la DGSI. Elle regroupe sur un même plateau des représentants de l'ensemble des services concernés, du premier ou du second cercle, qui sont connectés à leurs propres réseaux informatiques sécurisés, et permet de fusionner l'information qui intéresse la lutte antiterroriste sur le territoire national. Mais nous pourrions également citer la cellule Hermès, qui traite de sujets liés au renseignement et intéressant un ou plusieurs services.

Plus généralement, et c'est devenu la règle, lorsque plusieurs services ont un sujet commun d'intérêt, nous produisons des notes bi-timbres, tri-timbres ou multi-timbres, qui permettent d'avoir une approche plus globale et plus pertinente et de la partager. Nous sommes beaucoup plus efficaces à plusieurs que chacun isolément sur un même sujet. La démarche est particulièrement vertueuse.

Nous pouvons donc constater que les choses sont en train de changer, et que la culture interservices se met en place. Cette évolution est aussi portée par l'Académie du renseignement. Celle-ci permet non pas de former, au sens académique du terme, nos personnels puisque nous avons nos spécificités et nos propres centres de formation, mais de mettre en relation des représentants ou des stagiaires de chaque service, ce qui favorise une meilleure connaissance mutuelle et une meilleure interconnexion entre les services.

Ensuite, le fait de mutualiser nos capacités techniques, dont je vous ai parlé tout à l'heure, va renforcer la culture interservices. Quand on travaille sur les mêmes outils, il est beaucoup plus facile de communiquer et de se comprendre.

Ainsi, une vraie dynamique est en train de se développer, et cela va s'intensifier dans le futur. J'ajoute qu'au niveau tactique, des cellules un peu plus confidentielles ont été créées en interservices. Elles répondent à des problématiques très particulières sur lesquelles nous nous devons d'avoir une grande réactivité, ce que ne permet pas l'échange à un niveau supérieur.

La quatrième exigence est d'investir des champs nouveaux de confrontation que sont l'espace cyber et l'espace exo-atmosphérique.

Le fait d'une présence adaptée dans l'espace cyber constitue un vrai enjeu pour la DRM. Nous voyons tout le potentiel qu'il y a à exploiter le renseignement disponible sur le web, qu'on fusionnera ensuite avec des renseignements issus d'autres capteurs, images, électromagnétiques ou renseignements d'origine humaine.

Pour l'instant, l'approche est assez incrémentale. Nous avons créé en 2015, au sein de la DRM, le Centre de recherche et d'analyse cyber (CRAC) qui est dédié à la recherche dans le monde du web. Ce centre nécessite des compétences et des outils très particuliers. Nous considérons aujourd'hui que seulement 4 % des informations sur internet sont directement accessibles au travers des moteurs de recherche traditionnels comme Google. Mais nous nous intéressons à ce qui est beaucoup plus dissimulé – le *deep web* et le *dark web*, qui est encore plus caché. C'est une véritable mine de renseignements, à condition de savoir y accéder. Aujourd'hui, nous développons cette capacité, qui est très intéressante et prometteuse. Le CRAC emploie environ 90 personnes, et la future LPM devrait nous apporter quelques moyens supplémentaires.

Investir l'espace exo-atmosphérique constitue un autre enjeu.

De multiples acteurs sont impliqués : le Commandement interarmées de l'espace, dont vous avez auditionné le chef, et qui mène les opérations dans l'espace ; le Commandement de la défense aérienne et des opérations aériennes de l'armée de l'air, qui est chargé d'établir la situation spatiale ; et la DRM qui est chargée d'évaluer la menace spatiale à l'encontre de nos intérêts nationaux.

Grâce à des capteurs qui permettent de surveiller assez finement l'espace, nous savons qu'il s'y passe quelque chose. Aujourd'hui, pour vous donner un exemple très concret, des microsatellites gravitent autour de nos satellites les plus sensibles. Nous voyons bien que leur cinématique n'est absolument pas normale et qu'elle est suspecte, voire inamicale, de la part de certains pays.

Pour faire face à ces défis, la DRM a lancé un projet majeur et structurant pour dans les années à venir : l'innovation technologique.

La DRM a lancé le projet *intelligence campus* en 2015. Aujourd'hui, ce projet prend forme. Il sera structuré sous l'égide de l'initiative Innovation Défense du ministère des Armées. L'idée est de regrouper plusieurs acteurs sur la base de Creil : nos spécialistes du renseignement, nos experts, avec des chercheurs, des industriels et des *start-up*. Il s'agit de répondre à tous les défis qui s'offrent à nous en matière d'exploitation, notamment dans le traitement de l'image et la « Geo-Int » – c'est-à-dire du renseignement géo-localisé et géo-référencé – qui sont des pôles d'excellence et d'expertise de la DRM.

Comme je l'ai dit précédemment, ce projet est structuré en trois piliers : la formation, la recherche et l'innovation.

En 2020, le centre de formation interarmées au renseignement, le CFIAR, qui est aujourd'hui situé à Strasbourg, déménagera à Creil, l'objectif étant de le rapprocher de mes centres d'expertise. On pourra sans doute, de cette façon, dégager de fortes synergies. Ainsi, le CFIAR participera lui aussi à la montée en puissance d'*intelligence campus*.

Dans le domaine de la recherche, nous avons déjà passé un certain nombre de protocoles entre nos centres et plusieurs universités, écoles d'ingénieurs et centres de recherche, et nous allons poursuivre ces partenariats.

Toutefois, ce projet a longtemps été porté par la DRM seule. Nous allons l'ouvrir très rapidement aux autres services de renseignement. En effet, nous nous apercevons que, dans ce domaine, nous avons tous les mêmes besoins et les mêmes difficultés. Donc, ce qui pourra émerger comme solutions techniques et comme outils, notamment d'intelligence artificielle, issus de cette initiative *intelligence campus*, profitera aux autres services de renseignement.

Très concrètement, nous avons procédé à d'importants recrutements de personnels civils parce que nous n'avions pas cette capacité dans les armées, et ce recrutement va continuer sa montée en puissance, avec de nouveaux experts dans de nouveaux domaines. Les *data analysts* et les *data scientists*, vont notamment nous permettre d'évaluer les produits d'intelligence artificielle et de big data qui nous sont proposés. Toutes les semaines, une *start-up* ou une entreprise m'appelle pour me dire qu'elle a créé un outil formidable qui est la solution à tous mes problèmes ! Certes, les présentations Power Point font rêver. Mais, derrière, il faut que nous soyons capables d'évaluer ces outils et de les faire tourner sur des bases de données. Nous le ferons d'abord sur des bases de données fictives que nous aurons

créées pour protéger les nôtres tant que nous n'aurons pas d'assurance sur ce qui nous est proposé. Ensuite, nous ferons tourner ces outils en grandeur réelle pour pouvoir en mesurer la pertinence. Vous comprenez pourquoi j'ai besoin de cette expertise.

Mais l'innovation n'est pas contradictoire avec les programmes qui sont pensés au sein de la DGA, en particulier le projet Architecture de traitement et d'exploitation massive de l'information multi-service (ARTEMIS).

Ce n'est pas vraiment un outil, mais une architecture, une structure d'accueil qui va nous permettre d'intégrer ces différents outils dans différents domaines du renseignement pour nous aider à exploiter et analyser des données qui sont très hétérogènes – une image, une bande-son, une écoute, un papier, une carte, etc. Il faut être capable de fusionner tout cela pour en sortir une analyse pertinente.

Le projet ARTEMIS vise donc à fédérer tous ces outils et à les intégrer avec une architecture ouverte et souple, qui nous donnera cette capacité d'évolution qui est nécessaire dans ce milieu. Et toutes les initiatives qui seront lancées et qui aboutiront à des acquisitions d'outils se feront en lien étroit avec la DGA pour qu'à terme, ces outils puissent s'intégrer dans cette architecture globale ARTEMIS.

Pour conduire le projet *intelligence campus*, j'ai demandé à la DGA de me mettre à disposition un chef de projet. Le délégué a nommé l'ingénieur général de l'armement de première classe Caroline Gervais à mes côtés pour piloter ce projet et développer l'innovation au sein de la DRM en liaison étroite avec les initiatives lancées au sein de la DGA.

Je souhaiterais aborder maintenant avec vous nos ressources humaines, qui sont à la fois une richesse de la DRM, car nous avons des experts de très haut niveau, mais en même temps un point de vigilance dans le cadre de la loi de programmation militaire.

Entre 2013 et 2020, les effectifs de la DRM auront augmenté de 30 % – c'est la trajectoire telle qu'elle se précise aujourd'hui. Mais il faut poursuivre cette croissance, car les métiers de la DRM se transforment. Nous avons besoin d'experts, on nous demande toujours plus, on a de plus en plus de capteurs, on a toujours plus d'informations à exploiter, mais les effectifs des militaires spécialistes du renseignement n'ont pas évolué au même rythme.

Mon principal vivier d'experts se situe dans les armées. Je ne recrute pas moi-même de militaires. Les militaires de la DRM viennent des armées, donc de la fonction interarmées du renseignement, et font des allers et retours entre les armées et la DRM. Il est très important que l'augmentation des effectifs de la DRM et des unités de la FIR soit accompagnée d'une politique de recrutements d'officiers et de sous-officiers pour honorer ces nouveaux besoins. Il faut également savoir qu'il y a un important temps de latence entre le moment où nous décidons de recruter un sous-officier et son affectation effective dans les unités renseignement et que la formation des experts dans le domaine du renseignement prend du temps. Nous devons anticiper tout cela.

Je vous parlais tout à l'heure de mon rôle de « tête de chaîne » dans la fonction interarmées du renseignement. Une de mes principales préoccupations est de m'assurer que demain, la DRM et les armées auront les spécialistes dont elles auront besoin.

Certaines spécialités vont disparaître dans nos rangs. Par exemple, nous employons aujourd'hui des spécialistes très pointus dans le domaine de l'interception HF, qui avec des expertises particulières. Mais demain, les traitements seront automatisés et nous n'aurons plus besoin de ces expertises. En revanche, nous aurons besoin d'autres spécialistes, notamment les *data scientists* dont je vous parlais tout à l'heure.

Aujourd'hui, j'ai un vrai déficit en militaires. Encore une fois, il s'agit de spécialistes qui n'existaient pas avant dans les armées, qu'il nous faut recruter, former et dont il nous faut accroître le nombre. Aujourd'hui je compense – en tout cas partiellement – ce déficit par le recrutement de civils. Mais il y a déjà 30 % de civils à la DRM et il m'est très difficile d'aller au-delà, car je suis par ailleurs soumis à des contraintes de projection de personnels du renseignement sur les théâtres d'opérations, et que je ne peux pas y projeter de civils. Nous pouvons contourner le problème en leur faisant signer des contrats de réserve, qui leur permettent de partir en opération, mais la marge de manœuvre est limitée. Aujourd'hui, certains postes en opération ne sont pas honorés, faute de militaires disposant des bonnes compétences.

Nous devons donc recruter et, comme je l'ai déjà dit, travailler sur l'attractivité des métiers du renseignement. Compte tenu du contexte sécuritaire dans lequel nous vivons, nous n'avons pas trop de mal à recruter, du moins des spécialistes de haut niveau. Mais il est plus difficile de recruter des experts de catégorie B, et surtout de les fidéliser car ces experts sont très demandés dans le monde civil Souvent, ils viennent chez nous pour une première expérience, pour se faire un CV, puis ils vont chercher un autre emploi à l'extérieur. C'est un problème.

Aujourd'hui, le CNR-LT nous aide à travailler sur la mobilité interservices, pour proposer à chacun d'entre eux des parcours attractifs, valorisants et qualifiants. Même dans le domaine des RH, il faut faire preuve d'innovation et sortir des schémas traditionnels de recrutement et de déroulement de carrière. Nous devons construire des « boîtes à outils » innovantes en matière de recrutement, et combler nos carences avec d'autres types de contrats afin de faire face à ces missions, malgré la concurrence du monde civil. Nous avons de nombreux projets, et j'y reviendrai, si vous le voulez, à l'occasion des questions.

Nous nous intéressons aussi au télétravail, qui n'est peut-être pas assez exploité dans le domaine du renseignement. Tout n'est pas classifié dans ce que nous traitons, et un certain nombre de tâches peuvent être sous-traitées, notamment en télétravail. Nous travaillons, là encore, en lien étroit avec la direction des ressources humaines du ministère des Armées.

La dernière question que je souhaitais aborder est celle de la biométrie. Dans la nouvelle loi de programmation militaire, celle-ci fait l'objet d'une avancée notable, que nous appelions de nos vœux.

Jusqu'à présent, nous étions très contraints dans le domaine de la biométrie, dans la mesure où l'on ne pouvait faire de relevés biométriques que sur les personnes neutralisées ou capturées, ou sur les personnes que nous recrutons – les personnels civils de recrutement local (PCRL) – pour accomplir différentes tâches sur nos emprises en opérations.

Nous avons obtenu de pouvoir appliquer ces techniques de biométrie un peu plus largement à toute personne représentant une menace pour la sécurité de nos forces ou des populations civiles locales. Cela ouvre, par exemple, des perspectives d'identification de

terroristes qui se seraient dissimulés au sein de la population locale, à partir de traces relevées sur des engins explosifs ou des caches d'armes.

M. le président. La LPM n'est pas encore votée !

Général Jean-François Ferlet. Justement, nous anticipons son application. En effet, nous étudions actuellement la rédaction de directives, que nous appelons des « règles d'engagement », pour encadrer les prélèvements biométriques – sur qui, pourquoi, sur quels critères, avec quelles règles. Il ne s'agit pas de mettre en base de données biométriques toutes les populations, mais de définir des règles, au cas où la loi serait votée en l'état. Nous travaillons en lien avec la direction des affaires juridiques sur ces sujets. Si vous le souhaitez, nous pourrons y revenir au moment des questions.

M. le président. Je suppose que vous en aurez sur le sujet.

Général Jean-François Ferlet. Pour conclure, je reprendrai les idées-forces de mon exposé introductif.

Dans les années qui viennent, il faudra porter notre effort sur l'exploitation des renseignements. Nos capteurs sont extrêmement performants et reconnus par nos partenaires, mais l'exploitation est un vrai souci. Nous devons vraiment nous y atteler, pour ne pas être submergés par les données.

Il faut aussi investir des champs nouveaux, les nouveaux champs de bataille dont je parlais tout à l'heure : le domaine cyber, l'espace. Ces capacités sont encore en phase de montée en puissance mais elles sont très prometteuses.

Enfin, il faut veiller à un certain équilibre, en portant attention à la menace terroriste sans oublier, dans un contexte de retour des États-puissance sur la scène internationale, la surveillance et la veille stratégique, qui restent essentiels pour la DRM.

J'espère avoir été à peu près complet et clair. Je suis prêt à répondre à vos questions.

M. le président. Merci, Mon général. Nous commencerons par M. Loïc Kervran, qui siège à la Délégation parlementaire au renseignement.

M. Loïc Kervran. Merci, Mon général, pour cette présentation exhaustive. Je voudrais revenir sur les missions de la DRM.

Vous avez présenté comme un défi le maintien de l'équilibre entre veille stratégique et lutte antiterroriste. On pourrait aussi penser à l'appui direct aux forces en opérations, au *targeting* et aux *forensics* que vous avez évoqués.

Ensuite, on pourrait s'interroger sur votre champ de compétence géographique. En effet, on a appris récemment par la presse, à la suite de fuites relatives à l'attentat de Saint-Étienne-du-Rouvray, que la DRM avait émis des notes, notamment sur Adel Kermiche, à côté de beaucoup d'autres services qui travaillaient sur les mêmes personnes.

Enfin, vous avez évoqué l'excellence de la DRM en termes de renseignement d'origine image, et de renseignement d'origine électromagnétique. En revanche, vous avez

peu évoqué le renseignement d'origine humaine. La DRM a peut-être aussi des capacités en ce domaine, mais ne rencontre-t-elle pas, parfois, certaines difficultés pour traiter les sources, dans un système où le *turnover* est de quatre mois ? Le traitement des sources est sans doute assez différent de celui d'autres acteurs comme la DGSE, qui peuvent être présents sur les mêmes territoires.

Sur ces différents points, faudrait-il, selon vous, recentrer les missions de la DRM, pour qu'elle puisse continuer à contribuer de façon essentielle à la souveraineté et à l'indépendance de la France ? Je pense notamment au ciblage, ou *targeting*.

M. Fabien Gouttefarde. Ma première question concerne les effectifs. Loïc Kervran et moi-même avons rencontré d'autres services de la communauté du renseignement qui nous ont donné, dans le cadre de la future LPM, le nombre d'équivalents temps plein (ETP) qu'il était prévu de leur accorder. D'après le texte, entre 2019 et 2025, il y en aurait 1 500 pour toute la communauté du renseignement. Pouvez-vous nous donner votre chiffre, et la façon dont seront répartis ces effectifs supplémentaires ?

Ma seconde question concerne les moyens de surveillance, les systèmes spatiaux CERES – Capacité de renseignement électromagnétique spatiale – et MUSIS – *Multinational Space-based Imaging System*, c'est-à-dire, en français, système multinational d'imagerie spatiale. Pouvez-vous nous parler du calendrier de déploiement de ces appareils, de leur date de lancement, et de la plus-value de ces satellites ?

Mme Marianne Dubois. On sait qu'au Sahel, des alliances mouvantes se forment entre les différents groupuscules. Vous avez parlé tout à l'heure des linguistes. Est-ce vous arrivez à trouver les bonnes personnes ? Ces personnes sont-elles fiables ? Combien de temps vous faut-il pour analyser un renseignement, apprécier sa véracité et répondre ?

M. Fabien Lainé. Merci, Mon général, pour cet exposé exhaustif des missions et des enjeux de la DRM. Je voudrais revenir sur l'article 23 de la LPM et sur le fichier BIOPEX dont vous avez parlé tout à l'heure. De nombreux parlementaires s'interrogent. On comprend bien que pour renforcer les moyens d'investigation, il faut élargir le champ d'application des techniques biométriques, et que les prélèvements salivaires peuvent rendre bien des services. Vous avez dit qu'il ne s'agissait pas de mettre dans un fichier tous les paramètres biométriques de l'Afrique, et que vous réfléchissiez à des règles. Pouvez-vous nous en dire un peu plus ? Je pense que cela pourra éviter le dépôt de certains amendements.

M. Yannick Favennec Becot. Le volume des informations collectées augmente de façon exponentielle avec les avancées technologiques des satellites et des communications. Le traitement de ces données représente évidemment un véritable défi pour le renseignement militaire. L'intelligence artificielle devrait pouvoir analyser une grande partie des tâches actuellement assumées par les analystes. Mais dans quels délais ? Quelles sont vos attentes dans ce domaine ?

Par ailleurs, pensez-vous que la LPM soit suffisamment offensive pour tout ce qui concerne le renseignement dans l'espace ? Là encore, quelles sont vos attentes ?

M. Joaquim Pueyo. Le projet de LPM prévoit un effort notable concernant les personnels, avec la création de 1 500 postes supplémentaires entre 2019 et 2025. Il prévoit également l'acquisition de matériels, comme des avions de surveillance et de reconnaissance

stratégique. Enfin, dans le domaine spatial, des programmes doivent aboutir ; je pense au programme MUSIS et au système CERES

Vous avez démontré l'importance fondamentale du renseignement, tout en exprimant quelques inquiétudes par rapport à l'exploitation des données. Inutile en effet de mettre en place une logistique considérable si on ne sait pas exploiter celles-ci. Pensez-vous que les 1 500 postes qui seront créés à partir de 2019 seront suffisants pour pouvoir exploiter les données ? Quelle sera la qualité des personnels que vous allez recruter ? Vous nous avez dit en effet qu'il était difficile de les fidéliser.

M. le président. Cher collègue, il est prévu de recruter 1 500 personnes jusqu'en 2022, puis 1 500 par an – soit, au total, 6 000 personnes jusqu'en 2025.

Général Jean-François Ferlet. Faut-il recentrer les missions de la DRM ? Non. Nous devons remplir toutes nos missions – et c'est un « nous » collectif, je ne vise pas la DRM en particulier. Mais, encore une fois, nous devons veiller à maintenir des équilibres, et ne pas nous focaliser sur une seule menace, celle qui est la plus prégnante aujourd'hui, mais couvrir l'ensemble du spectre, pour ne pas être surpris par une menace qui pourrait émerger et que nous n'aurions pas vu venir.

Une commission d'enquête a été mise en place après l'attentat de Saint-Étienne-du-Rouvray, et je m'y rendrai cet après-midi.

Plus globalement, comme je le disais tout à l'heure, il est facile d'aller fouiller *a posteriori* dans des bases de données quand on sait ce que l'on cherche. Je vous ai d'ailleurs parlé du risque de se faire submerger par les données. Nous pouvons avoir des informations dans une base de données, sans être capable de trouver l'information pertinente au bon moment. C'est tout l'enjeu des outils d'intelligence artificielle que nous devons développer. Ce ne sont pas les RH, seules, qui régleront le problème. Nous devons donc nous doter de ces outils, qui nous permettront de faire des analyses plus pertinentes.

M. Loïc Kervran. Pourquoi la DRM travaillait-elle sur cette chaîne, comme beaucoup d'autres services qui, eux, travaillent plutôt sur le territoire national ?

Général Jean-François Ferlet. Chacun de nous a un périmètre d'action bien défini. Nous ne travaillons pas sur le territoire national. En revanche, lorsque nous travaillons sur des djihadistes à l'étranger, compte tenu des nouvelles technologies, des réseaux sociaux et des interconnexions entre les djihadistes du monde entier, il arrive que nous tombions sur des personnes qui ont des liens avec d'autres personnes qui vivent ou vont retourner en France.

La règle qui est appliquée systématiquement aujourd'hui sur ce type de cas est très simple et elle est la suivante : transmettre immédiatement le renseignement que nous trouvons– même si ce n'est pas dans notre mission – au service de renseignement qui pourrait en avoir besoin ; en l'occurrence, la DGSI. De la même façon, si nous trouvons des informations sur des comptes bancaires de terroristes dans le Sahel, nous les transmettons à TRACFIN. Et, dans le doute, nous le donnons quand même. Cela n'arrange pas forcément les autres services de renseignement, qui rencontrent les mêmes problèmes que moi en matière de gestion des données.

J’en viens aux capteurs ROHUM – acronyme de « renseignement d’origine humaine ». Le traitement des sources est effectivement une activité très sensible. Nous avons des capacités dans les armées et dans chaque service. Moi-même, je suis plutôt en interaction avec ce que fait la DGSE à l’étranger, puisque nous travaillons, nous aussi, essentiellement à l’étranger. Voilà pourquoi le traitement des sources est coordonné, sur les théâtres, avec la DGSE. Nous faisons bien attention à ne pas traiter deux fois la même source, au risque de perturber l’action de l’un ou de l’autre, voire de se faire instrumentaliser.

Vous avez évoqué la difficulté que représente l’important *turnover* des militaires en opérations extérieures – en général, quatre ou six mois. Malgré tout, nous ne pouvons pas fonctionner autrement. Il a donc fallu faire en sorte de pallier cet inconvénient.

Nous avons des régiments spécialisés sur les théâtres d’opérations, en auto-relève, dans le traitement des sources humaines. Nos militaires restent effectivement quatre ou six mois en OPEX. Voilà pourquoi, quatre mois avant de partir en opération, l’équipe qui va être projetée travaille déjà en France sur la connaissance des sources et est en contact permanent avec l’équipe déjà en place sur le théâtre. C’est comme si elles formaient une seule équipe : une partie est sur le terrain, l’autre partie travaille en arrière-plan et sera ensuite projetée. Cette préparation intellectuelle permet de disposer de plusieurs années d’historique sur le traitement de ces sources. Et cela donne entière satisfaction avec de beaux résultats opérationnels. Je n’ai pas entendu qu’on se soit plaint de la façon dont nous traitons nos sources. Bien au contraire.

J’ai également été interrogé sur la répartition des effectifs. Pour la période 2019-2022, la DRM devrait bénéficier directement de 90 personnels supplémentaires sur un total de 1 500, et 211 personnels de plus seront dévolus aux unités spécialisées de renseignement des armées sur lesquelles la DRM s’appuie. L’effort total sera donc d’environ 300 personnels.

M. Joaquim Pueyo. Cela correspond à vos besoins ?

Général Jean-François Ferlet. Personne ne vous répondra jamais qu’il a assez de personnel ! Cela dit, mon objectif n’est pas de grossir pour grossir. Je dis toujours que je ferai au mieux avec ce que l’on me donnera. Mais on n’en a jamais assez.

M. le président. Maintenant, il y a l’intelligence artificielle !

Général Jean-François Ferlet. Cela demande aussi du personnel supplémentaire, de nouvelles expertises et compétences.

Vous parliez de l’arrivée de nouveaux systèmes : lorsque nous lançons un nouveau programme, il y a ce que j’appelle des « incontournables ». Prenons l’exemple de la mise en service de MUSIS et de celle de CERES, qui interviendra immédiatement après : au-delà des satellites, il y a des segments sol avec des stations sol, de l’exploitation, et des personnels derrière les consoles. Et si l’on peut penser que MUSIS, qui remplace Helios, bénéficiera d’un transfert d’une grande partie de son personnel, il n’en sera rien pour CERES qui constitue une nouvelle capacité. Actuellement, le système ELISA – pour *Electronic Intelligence Satellite* –, programme d’études en amont de CERES, compte un nombre limité de personnels pour son exploitation expérimentale. Avec CERES, on nous livre une vraie capacité nouvelle qui a

nécessité un important effort financier du ministère. Je vais donc consacrer une partie de ces nouvelles ressources humaines à l'exploitation de CERES.

MUSIS succède à Helios. Le premier satellite doit être lancé au mois de décembre prochain. En général, le calendrier des programmes spatiaux est respecté car les créneaux de tir sur Ariane doivent être réservés. Un deuxième satellite doit être lancé l'année suivante. Ce programme est mené en coopération avec plusieurs partenaires européens, qui disposeront d'un droit de tirage. L'Allemagne est un acteur important de ce programme puisqu'elle a participé au financement du troisième et dernier satellite.

MUSIS offrira une résolution bien meilleure que celle d'Helios 2 et garantira aussi une meilleure agilité. L'agilité se définit comme le temps de réaction entre la programmation du satellite et le nombre de zones qu'il est capable de couvrir simultanément. Nos zones d'intérêt sont souvent assez concentrées géographiquement au Moyen-Orient. Aujourd'hui, l'agilité des satellites est toute relative. Un seul passage ne permet pas toujours de traiter tous les points que l'on a sélectionnés. MUSIS sera beaucoup plus agile et permettra de traiter beaucoup plus d'objectifs lors d'un même passage.

Vous avez évoqué le Sahel et les linguistes. Nous avons effectivement un souci avec les linguistes pour certaines langues. Je prendrai l'exemple emblématique du tamasheq. Le tamasheq est parlé par les Touaregs, dont est issu le noyau dur des groupes terroristes que nous rencontrons dans le Sahel. Le tamasheq n'est pas une langue unique : il comporte de nombreux dialectes un peu différents selon les régions, car nous trouvons des Touaregs en Mauritanie, au Mali, en Algérie, au Niger ou en Libye. Les locuteurs du tamasheq sont difficiles à recruter. En général, il s'agit de Touaregs qui ont encore des attaches familiales au Sahel. Ces candidatures sont, comme tous les personnels civils et militaires du ministère, transmis à la direction du renseignement et de la sécurité de la défense (DRSD) pour les habiliter au niveau de sécurité idoine.

Nous fondons quelques espoirs sur les outils d'intelligence artificielle, comme les traducteurs automatiques mais, sachant qu'aujourd'hui ces dispositifs ne sont pas très fiables dans des langues courantes comme l'anglais, nous n'attendons pas de bons résultats pour demain avec une langue rare aux dialectes multiples.

La question du recrutement pour la traduction des langues rares constitue bien une difficulté récurrente. Nous essayons évidemment de mutualiser nos ressources avec les autres services. Cette situation nécessite de pas vouloir tout traduire, mais de bien cibler les interceptions qui nous semblent intéressantes et que l'on voudrait traduire, à l'aide de mots-codes ou de mots-clés.

Le temps nécessaire à l'exploitation des données est extrêmement variable. Elles peuvent être prises en compte immédiatement. Le Transall C-160 Gabriel recueille du renseignement en pratiquant des écoutes : le linguiste est dans l'avion, il écoute en direct, et s'il entend quelque chose d'intéressant, il note l'information et la diffuse immédiatement. Par ailleurs, nous disposons de beaucoup d'informations dans les bases de données. Tout n'est pas traduit. Ces informations peuvent faire l'objet de recherches ultérieures pour des études plus fouillées sur des sujets spécifiques.

Quelles règles appliquons-nous s'agissant des prélèvements destinés à des analyses biométriques ? Les règles d'engagement, dont je vous ai déjà parlé, serviront à cadrer

finement les choses sur le terrain. La biométrie est un outil très utile, mais il faut trouver un juste milieu dans l'usage que nous pouvons en faire, à la fois pour des raisons de principe et d'organisation.

Nous réfléchissons donc actuellement à ces sujets avec nos opérationnels et avec la direction des affaires juridiques afin de voir comment nous pouvons mettre en œuvre cette capacité intelligemment et avec discernement. Il faut bien garder à l'esprit que cette mesure est destinée à réduire le niveau de menace contre nos forces et la population civile locale en permettant une identification fiable de certains individus ayant des antécédents.

Évidemment, les fichiers seront déclarés de manière transparente.

Que pouvons-nous attendre de l'intelligence artificielle pour le traitement des données, et dans quels délais ? Nous ne partons pas de rien. Nous disposons déjà d'outils développés dans le cadre de la recherche technique pour exploiter les données disponibles dans nos *data centers*.

Nous mesurons bien l'immense potentiel de ce secteur, et nous savons que les armées ne sont pas toujours en avance dans ce domaine par rapport au milieu civil. Lorsque vous passez au rayon cuisines d'une grande surface ou que vous faites quelques recherches sur le sujet sur internet et que votre smartphone vous envoie personnellement, le lendemain, des publicités vous proposant une cuisine neuve, c'est le résultat de la collecte d'une multitude de données – vous avez accepté d'être localisé et validé l'utilisation de *cookies*… Vous imaginez la taille des bases de données connectées au niveau mondial qui se trouvent derrière cela ! Des entreprises se consacrent d'ailleurs à la seule activité consistant à collecter et à revendre ces bases de données à des fins commerciales. D'autres les achètent et utilisent des outils extrêmement puissants pour les traiter et cibler individuellement ceux qui présentent un intérêt commercial. Les armées n'en sont pas là. Nous ne disposons pas d'outils aussi puissants, et nous n'avons pas la puissance financière nécessaire.

Aujourd'hui, même les États sont dépassés par la puissance financière de certaines entreprises, comme Microsoft ou Google, qui peuvent consacrer à ces évolutions des moyens bien supérieurs.

Quoi qu'il en soit, nous n'allons pas développer de notre côté des outils qui existent déjà sur le marché. Il ne s'agit que d'instruments qui pourront répondre directement à nos besoins après avoir fait l'objet d'adaptations ou de paramétrages particuliers. Nous devons les acquérir en boucle courte, sachant qu'ils sont en évolution rapide et permanente.

La LPM nous permettra-t-elle de disposer des effectifs suffisants pour exploiter les données ? Je l'ai dit, ce ne sera jamais suffisant, mais nous ne comptons pas seulement sur les effectifs pour exploiter les données. Ils sont cependant indispensables pour que nous disposions d'experts, et pour utiliser les outils adéquats.

M. le président. Mes chers collègues je vous invite à la concision car quatorze d'entre vous souhaitent encore interroger le général. Nous commençons par le rapporteur pour avis de la commission des Lois sur la LPM.

M. Jean-François Eliaou. L'espace cyber fait l'objet de contraintes légales et normatives. Tant sur le plan de la cyberdéfense que de la cyberattaque, comment voyez-vous

les choses en termes de personnels et d'actions ? Sur le territoire national, ces dernières sont encadrées par des textes qui n'ont pas toujours leur équivalent à l'extérieur.

La base biométrique BIOPEX est actuellement en construction. Le recueil des données suppose que les personnels soient formés, et leur utilisation implique le croisement des fichiers. Quel est votre sentiment à cet égard ?

Mme Frédérique Lardet. Général, vous avez cité dans vos propos liminaires le projet *intelligence campus* de Creil. Il s'agit du premier écosystème européen civil et militaire en traitement de la donnée, d'une pépinière d'entreprises, mixant *start-up* et PME innovantes, dont l'ambition était ou est de devenir le premier centre européen de traitement des données à vocation civile et militaire.

Une information circule toutefois selon laquelle ce projet serait fragilisé par manque de soutien financier. Pouvez-vous nous confirmer ces rumeurs ? Le cas échéant, quelles précisions pouvez-vous apporter, et des moyens seront-ils accordés pour soutenir cette structure qui, à ce jour, reste associative ?

M. Claude de Ganay. Le 5 février dernier, lors d'une rencontre avec l'association des journalistes de défense, vous avez déclaré en parlant du Sahel : « *Si l'on regarde le nombre d'attaques, on ne peut pas parler de dégradation sécuritaire. Il y a un bruit de fond de harcèlement, mais qui existe depuis la fin de Serval et qui continue.* » Vous avez même ajouté : « *La situation n'est pas satisfaisante, mais elle est contrôlée.* »

J'avoue que ces propos m'ont un peu surpris : le Mali est virtuellement coupé en deux par l'insurrection des Peuls, au centre du pays, qui déborde au Burkina Faso, tandis que Groupe pour le soutien de l'islam et des musulmans – GSIM ou *Jamaat Nosrat al-Islam wal-Mouslimin (JNIM)* – d'Iyad ag-Ghali continue de harceler les forces internationales dans le nord, et que les forces armées maliennes ne sont toujours pas en mesure de contrôler seules leur territoire. Pourriez-vous expliciter vos propos du mois de février ?

M. Olivier Becht. Mon général, vous avez insisté sur l'importance des puissances de calcul à la fois pour le traitement des données, mais également pour la cryptologie. Que pensez-vous des efforts d'investissement de la France dans le quantique, que ce soit en faveur des calculateurs ou des ordinateurs quantiques ?

Vous avez également insisté sur notre dépendance et notre fragilité par rapport au réseau satellitaire. Que pensez-vous des moyens de résilience, y compris humains, dans l'hypothèse d'une neutralisation de ces outils ?

M. Philippe Michel-Kleisbauer. Vous avez évoqué vos difficultés pour recruter des personnels pour certaines missions, et l'impossibilité de recourir à des non-militaires. Ce problème est-il insurmontable ? Des civils, qui pourraient être formés, sont peut-être prêts à exercer ces missions. Ne pourrions-nous pas imaginer ensemble le cadre législatif dont vous auriez besoin pour cela ?

Mme Nicole Trisse. Quel est le pourcentage de femmes dans vos effectifs, et dans quels domaines sont-elles employées plus particulièrement ? Si vous me répondez « secrétariat et café », ça ne va pas le faire ! (*Sourires*.)

M. le président. Madame Trisse, vous n'avez pas vraiment le droit de faire aussi les réponses.

Mme Nicole Trisse. C'était seulement une menace, Monsieur le président…

Mme Françoise Dumas. Au regard de l'évolution des comportements des États-puissances, quelles sont plus précisément les compétences qui manquent encore à votre service ? Quelles sont les marges de progression en termes de coordination de l'ensemble de vos services ?

J'ai pu me rendre à Gao, sur un théâtre d'opérations, et j'ai pu mesurer combien, au-delà de la disponibilité de vos personnels, chaque activité était susceptible d'apporter du contenu à exploiter – je pense en particulier à l'aide médicale aux populations.

Général Jean-François Ferlet. Je ne veux pas esquiver la question relative aux contraintes normatives en matière de cyber offensif et défensif, mais, en clair, ce n'est pas dans mon domaine de responsabilité. La DRM ne fait que du renseignement dans ces espaces. La lutte informatique est dévolue à d'autres organismes – notamment au Commandement de cyberdéfense (COMCYBER). Pour ce qui nous concerne, nous ne faisons que capter du renseignement dans l'espace cyber : pour nous, il s'agit d'un média comme un autre.

Je ne fais que du renseignement d'intérêt militaire en appui des opérations : je m'intéresse aux médias utilisés par Daech ou par Al-Qaïda. Évidemment, parfois, nous récoltons une information qui peut intéresser la DGSI, et nous la lui transmettons. Ni la lutte offensive ni la lutte défensive ne sont dans le périmètre de la DRM.

Le développement de la biométrie demande en effet de former les personnels. Nous ne partons pas de zéro car nous sommes déjà autorisés à effectuer des relevés sur des personnes capturées ou des employés locaux. De plus, nous coopérons avec l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) dont les compétences et le savoir-faire en la matière sont reconnus et nous travaillons avec eux pour bénéficier de leur expérience dans le traitement des données. Il n'y aura pas de connexion des bases de données, car nous disposons des nôtres sur BIOPEX dont le périmètre de recueil est limité aux opérations extérieures.

Intelligence campus n'est, à l'heure actuelle, qu'un concept. Nous avons signé certaines conventions relatives aux piliers « formation » et « recherche » avec des organismes du monde académique et de la recherche. Je ne pense pas que le problème réside aujourd'hui dans un manque de soutien financier : les freins à l'innovation ne sont pas de cette nature. Ils sont plutôt liés au code des marchés publics et à la question de l'accès à nos bases de données, qui sont très sensibles – du point de vue de la sécurité des systèmes d'information (SSI), on ne pourrait pas permettre d'y accéder. Dans un premier temps, le principal intérêt d'*intelligence campus* est, à mes yeux, d'aider à identifier très concrètement les freins. Par la suite, il se peut que nous ayons à vous solliciter pour des évolutions sur certains points. Il ne faut pas se fixer comme critère le risque zéro, car il n'existe pas, mais plutôt un risque maîtrisé. On doit se demander quels risques on court, quelles sont les conséquences si ça se passe mal et, en contrepoint, quels gains on attend. Nous le faisons en permanence dans le cadre de nos opérations, mais ce n'est pas l'approche qui prévaut en matière de SSI ou sur le plan réglementaire : on a au contraire une approche reposant sur le risque zéro, ce qui conduit à se fixer des interdits.

Mes propos sur le Sahel m'ont valu beaucoup de coups de fil… J'ai passé un an dans cette région, et je sais parfaitement quelle était la situation sécuritaire entre 2014 et 2015. Les djihadistes nous harcèlent, mais cela s'inscrit dans la continuité. Si l'on regarde le nombre d'attaques sur trois ans, mois par mois, quel qu'en soit le type – attaques directes ou indirectes, usage de mortiers ou des *Vehicle Borne Improvised Explosive Devices* (VBIED), embuscades… –, le bruit de fond est le même. Ce n'est pas une situation satisfaisante, et je ne conseillerais à personne d'aller faire du *trekking* à Tessalit, mais on ne peut pas parler de dégradation sécuritaire, objectivement.

Certains éléments nous font penser, néanmoins, que la tendance n'est pas bonne. Si le nombre d'incidents sécuritaires n'augmente pas, nous constatons néanmoins un déplacement vers le Sud, dans une région beaucoup plus peuplée, notamment par les Peuls, où le potentiel de déstabilisation est plus important que celui causé par quelques Touaregs djihadistes en plein désert. La population peule n'a pas des revendications spécifiquement djihadistes : elle est davantage traversée par un sentiment de frustration ou par l'impression d'être maltraitée par le pouvoir central, à Bamako : s'il peut y avoir des ralliements à des groupes djihadistes, c'est plutôt par dépit ou pour d'autres motivations qui ne sont pas fondamentalement djihadistes.

Nous avons toujours dit que la menace sécuritaire, compte tenu de son niveau, serait à la portée de nos partenaires si l'on arrivait à les faire monter en puissance. Dans l'ensemble du Sahel, qui représente quand même neuf fois la superficie de la France, le noyau dur est compris entre 450 et 500 djihadistes – auxquels il faut ajouter des intermittents, si je puis dire, qui peuvent poser une mine contre un billet. C'est à la portée des forces locales, à condition qu'elles s'organisent en conséquence et qu'il y ait une volonté de travailler ensemble.

Si votre question était de savoir si l'on se trouverait dans une situation difficile en cas de perte de tous nos satellites, la réponse est évidemment « oui ». Les satellites sont vulnérables par nature : il est plus facile de les attaquer que de les défendre, car on ne va pas les blinder – sinon, le coût serait considérable, la mise en orbite se payant au poids. Un des moyens de contournement auxquels nous réfléchissons, comme les Américains, consiste à envoyer des essaims de satellites, beaucoup plus petits et orbitant plus bas, au lieu d'utiliser seulement deux ou trois satellites de taille plus importante pour assurer la même couverture. On obtiendrait un résultat plus résilient car l'ensemble serait plus difficile à neutraliser. Rencontrons-nous des difficultés pour recruter des civils en raison de la législation actuelle ? Nous n'avons pas suffisamment exploré toutes les possibilités existantes, comme le recours à la sous-traitance ou à des vacataires. Je dispose déjà de russophones, par exemple, au sein de la DRM et de la FIR, mais je peux avoir un besoin ponctuel pour une étude particulière, nécessitant une analyse très importante de documents et de données : dans ce cas, je ne vais pas demander un ETP supplémentaire pour embaucher quelqu'un. Nous pourrions notamment pré-identifier – et pré-habiliter – des contractuels auxquels nous serions susceptibles d'avoir recours pour des missions ponctuelles, dans le cadre de missions d'intérim. C'est une des pistes pour compléter notre boîte à outils. Je l'ai dit : j'ai lancé en interne un chantier relatif aux ressources humaines et je souhaite que l'on fasse preuve d'audace et d'innovation.

Nous comptons 27 % de femmes dans nos rangs, ce qui est largement au-dessus de la moyenne dans les armées. Dans l'armée de l'air, dont je suis issu, le taux s'élève à 22 %, ce qui est déjà assez élevé. Les raisons sont assez simples. Il y a d'abord la question des aspirations : les femmes sont plus facilement intéressées par nos métiers que par d'autres, un

peu plus rudes, dans les armées. Par ailleurs, les capacités physiques ne nous intéressent pas dans le monde du renseignement, ce qui permet une parfaite égalité des chances. Quand nous recrutons, nous regardons seulement les compétences, sans nous préoccuper du sexe des candidats.

Il y a beaucoup de femmes chez nous, mais elles sont réparties assez inégalement : elles sont nombreuses, par exemple, parmi les analystes. C'est une question d'appétence : pour les postes de sous-officiers spécialisés dans des domaines très techniques, que j'ai évoqués tout à l'heure, j'ai moins de femmes candidates, car cela les intéresse moins. En revanche, la chef de projet d'*intelligence campus* est une ingénieure générale de l'armement, et une femme est aussi à la tête du CRAC, le centre cyber qui est en pleine expansion. À partir du moment où les capacités physiques n'ont pas d'importance dans mon service, il n'y a pas de sujet. Au sein de la FIR, on ne trouvera pas beaucoup de femmes, par exemple, au sein du 13e régiment de dragons parachutistes (RDP), qui est spécialisé dans la recherche en profondeur : les missions y sont très physiques.

J'ai parlé tout à l'heure des compétences : nous devons réaliser des efforts en ce qui concerne les nouveaux métiers, comme les *data scientists*, et en particulier les géomaticiens. Ces derniers sont capables de modéliser des données géographiques en les croisant avec d'autres éléments afin de produire de la Geo-Int, ou *geospatial intelligence*. En combinant des données hétérogènes, mais toutes géoréférencées, on obtient de nouveaux produits qui sont très appréciés : nous avons désormais des cartes interactives sur lesquelles on peut cliquer, et qui ont été élaborées directement à partir des bases de données. On entre dans une autre dimension, qui nécessite de nouvelles compétences. Nous manquons d'experts pour l'exploitation des données, et il faut donc monter en puissance.

Quelles sont les marges de progrès pour la coopération interservices ? Elles existent toujours, mais il y a une vraie dynamique dans ce domaine. Quand nous fournissons des éléments à la DGSE, je n'ai pas à le valider : les échanges ont lieu tous les jours au niveau des traitants ou des cellules interservices créées sur des sujets particuliers. On est très loin d'éventuels blocages ou jeux d'intérêt au niveau supérieur : les connexions se font par le bas, de manière quotidienne.

Quant à l'importance des capteurs, je rappelle que le renseignement est élaboré à partir de différentes sources. Le renseignement humain est essentiel, et la technologie ne doit pas nous le faire oublier. Le contact avec les populations locales, par des actions de soutien sanitaire et médical, y participe : les gens nous parlent quand ils sont en confiance. Tout cela contribue à une meilleure connaissance et à une meilleure appréciation de la situation sur le terrain, ce qui est très important.

M. le président. Nous passons à une dernière série de questions, en commençant par M. Olivier Gaillard, rapporteur pour avis de la commission des Finances sur la LPM.

M. Olivier Gaillard. Une nouvelle course à l'armement se joue, celle de l'intelligence artificielle, dont vous avez largement fait état. Il faut sans doute se préparer à la robotisation du renseignement. Dans ce domaine, la LPM pose-t-elle vraiment les jalons nécessaires ?

Mme Laurence Trastour-Isnart. J'aimerais savoir combien de temps prend la formation des personnels que vous avez recrutés et comment vous faites ensuite pour les fidéliser.

M. Christophe Lejeune. Vous avez évoqué votre contribution à la dissuasion nucléaire. S'agissant de pays étrangers, votre mission consiste-t-elle, notamment, à évaluer le niveau de compétence atteint, la crédibilité de la menace et les évolutions technologiques ?

Mme Sereine Mauborgne. J'ai une question d'ordre pratique, mais qui pose aussi un certain nombre de problèmes sur le plan juridique : en ce qui concerne la collecte de renseignements, en particulier biométriques, dans la bande sahélo-saharienne, quelle est l'articulation avec la protection de notre territoire ? Il faut éviter que certains individus pénètrent sur notre sol.

M. Thibault Bazin. Parmi les freins à l'innovation, vous avez cité la protection du secret et une approche reposant sur le risque zéro. Afin de remplir vos missions, notamment de protection, auriez-vous besoin d'une évolution de la loi du 30 octobre 2017 ? Vous avez déclaré que ce n'était pas encore « mûr », mais ce serait peut-être le cas si l'on vous aidait.

M. Jean-Michel Jacques. Sur le plan technologique, vous avez parlé de « cycles courts » pour le matériel dont vous avez besoin. Créez-vous des laboratoires communs entre des PME et l'ensemble des services de renseignement français pour essayer de favoriser les liens et l'émergence de l'innovation ?

M. Philippe Chalumeau. Ma question porte sur *intelligence campus*. Vous avez évoqué la constitution de *data centers* : seront-ils répartis sur le territoire ou concentrés à Creil ?

Général Jean-François Ferlet. Je crois qu'il ne faut pas tout attendre de la LPM. La course à l'intelligence artificielle et l'acquisition de capacités en la matière ne sont pas uniquement une question de moyens financiers. C'est une affaire d'innovation : dans ce domaine qui évolue extrêmement vite, on doit donc penser autrement. Les processus habituels d'acquisition pour les programmes d'armement ne sont pas adaptés, car on ne va pas assez vite. L'idée est de faire autrement, d'où *intelligence campus* et le projet « Innovation Défense ». Une demande a été adressée à la DGA, et elle s'organise en conséquence. La nécessité de consentir des efforts est reconnue partout, y compris dans la Revue stratégique, et il faut maintenant avancer concrètement.

En réponse à la question relative aux freins, je pense que l'on n'a pas nécessairement besoin de légiférer sur tout ; ce sont parfois les mentalités qui doivent évoluer. Souvent, ceux qui nous contrôlent, ou nous donnent des avis, nous signalent un risque et nous recommandent de ne pas le prendre. Certains sont payés, au contraire, pour décider et pour prendre des risques, après les avoir évalués et en les maîtrisant. Pour ma part, je suis prêt à prendre des risques dans ce cadre. Je l'ai dit, le risque zéro n'existe pas.

La création de laboratoires communs correspond tout à fait au concept qui est à la base d'*intelligence campus*. La DGSE et la DRSD y seront associées : ce n'est pas seulement un outil développé par la DRM pour elle-même, mais pour la communauté du renseignement, au sens large du terme, c'est-à-dire au-delà du ministère des Armées. Dans un premier temps, le projet est porté par ce ministère, car il faut bien que quelqu'un le fasse. Si l'on se place tout

de suite dans un cadre interministériel, on n'avancera pas, car plus on est nombreux autour de la table, moins on y arrive. C'est pourquoi le projet commence avec la DRM et ses partenaires au sein des services de renseignement du ministère des Armées. Nous ferons, bien sûr, bénéficier les autres services des résultats, mais nous ne voulons pas, pour l'instant, qu'ils donnent un avis sur ce que nous faisons ou sur la manière de procéder. À terme, il serait opportun que ce genre d'outils existe au niveau interministériel, mais nous n'avons pas intérêt à ce que ce soit le cas au démarrage.

Que faisons-nous en matière de recrutement, de formation et de fidélisation ? Nous ne rencontrons pas de problème de recrutement, car nous sommes assez attractifs, même si nous avons des concurrents en interne, au sein des services de renseignement : certains savent mieux rémunérer leurs agents que nous. Ils versent notamment des primes dites de « confidentialité » – comme si la DRM n'avait pas, elle aussi, des contraintes en la matière. C'est une des questions sur lesquelles nous travaillons dans le cadre du CNR-LT : nous regardons comment améliorer la mobilité interservices dont je parlais tout à l'heure, en revoyant un peu tous les statuts pour essayer d'arriver à un équilibre en matière d'attractivité. Cela contribuera aussi à une meilleure coopération interservices. En ce qui concerne la fidélisation, nous nous efforçons de travailler sur les difficultés que j'ai évoquées tout à l'heure. Notre vrai point fort réside dans l'intérêt du travail et dans les profils de carrière que nous pouvons proposer. Un spécialiste de la SSI ou des réseaux peut aller travailler dans une banque, mais ce sera toujours moins intéressant que chez nous.

Quelle est la contribution de la DRM à la contre-prolifération ? Tous les aspects que vous avez cités font partie de nos missions, lesquelles sont exercées en lien avec la DGSE. Dans le domaine de la prolifération nucléaire, par exemple, la capacité d'un pays dépend du développement de l'arme elle-même, mais aussi de sa miniaturisation – elle doit être suffisante pour que la charge entre dans un vecteur, en général un missile balistique. On doit donc suivre non seulement les programmes nucléaires, en particulier la capacité à produire la matière fissile, comme le plutonium, mais aussi les programmes balistiques, en s'intéressant à la portée et à la fiabilité des vecteurs. Il faut maîtriser toute une chaîne de savoir-faire pour obtenir une capacité nucléaire opérationnelle, et chacun de ces savoir-faire particuliers entre dans le cadre de la lutte contre la prolifération et le transfert de technologies. Un autre pan de notre travail est le soutien à notre propre dissuasion. Sa crédibilité dépend de la performance de notre armement, mais aussi des défenses. Il faut que nos armes arrivent à destination sans être détruites en cours de route. Nous comparons les évolutions avec les capacités de pénétration de nos propres missiles balistiques et de notre vecteur aérien, afin de déterminer si notre dissuasion est crédible et si la future génération le restera.

Quelle est l'articulation entre BIOPEX et les fichiers nationaux ? Je l'ai dit : il n'y a pas d'interconnexion, pour des raisons légales. À l'heure actuelle, si la DGSE ou la DRSD, par exemple, nous interrogent, nous leur répondons instantanément. S'il n'existe pas d'interconnexion physique, il y a en revanche un échange de renseignement fluide, en réponse à des requêtes.

M. le président. Merci, Mon général, pour toutes ces précisions.

La séance est levée à dix-heures cinquante-cinq.

*

* *

Membres présents ou excusés

Présents. - M. François André, M. Thibault Bazin, M. Olivier Becht, M. Jean-Jacques Bridey, Mme Carole Bureau-Bonnard, M. Philippe Chalumeau, M. Jean-Pierre Cubertafon, Mme Marianne Dubois, Mme Françoise Dumas, M. M'jid El Guerrab, M. Yannick Favennec Becot, M. Jean-Jacques Ferrara, M. Jean-Marie Fiévet, M. Claude de Ganay, M. Thomas Gassilloud, M. Fabien Gouttefarde, Mme Émilie Guerel, M. Jean-Michel Jacques, M. Loïc Kervran, M. Fabien Lainé, Mme Frédérique Lardet, M. Christophe Lejeune, Mme Sereine Mauborgne, M. Philippe Michel-Kleisbauer, Mme Patricia Mirallès, Mme Josy Poueyto, M. Joaquim Pueyo, M. Gwendal Rouillard, Mme Laurence Trastour-Isnart, Mme Nicole Trisse, M. Stéphane Trompille

Excusés. - M. Bruno Nestor Azerot, M. Florian Bachelier, M. Luc Carvounas, M. André Chassaigne, M. Stéphane Demilly, M. Olivier Faure, M. Richard Ferrand, M. Marc Fesneau, M. Laurent Furst, Mme Séverine Gipson, M. Christian Jacob, M. Jean-Christophe Lagarde, M. Jacques Marilossian, Mme Natalia Pouzyreff, M. François de Rugy, Mme Sabine Thillaye, Mme Alexandra Valetta Ardisson

Assistaient également à la réunion. - M. Jean-François Eliaou, M. Olivier Gaillard