ASSEMBLÉE NATIONALE

XV^e LÉGISLATURE

Mardi
27 février 2018
Séance de 15 heures

Compte rendu n° 41

SESSION ORDINAIRE DE **2017-2018**

# Compte rendu

## Commission de la défense nationale et des forces armées



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

*La séance est ouverte à quinze heures.*

**M. le président Jean-Jacques Bridey.** Nous sommes réunis cet après-midi pour auditionner le général Olivier Bonnet de Paillerets, commandant de la cyberdéfense, sur le projet de loi de programmation militaire (LPM). Nous sommes également heureux d'accueillir au sein de notre commission M. Olivier Gaillard, rapporteur pour avis de la commission des Finances, et M. Jean-François Eliaou, rapporteur pour avis de la commission des Lois. Nous avons déjà auditionné sur ce sujet de la cyberdéfense le secrétaire général de la défense et de la sécurité nationale (SGDSN) ; nous auditionnerons la semaine prochaine le directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

**Général Olivier Bonnet de Paillerets, commandant de la cyberdéfense.** Monsieur le président, Mesdames et Messieurs les députés, je suis très honoré d'être aujourd'hui devant vous. J'ai pris le commandement de cette entité cyber le 1er septembre 2017 à la suite de la création de cette nouvelle structure placée auprès du chef d'état-major des armées. J'ai passé vingt ans dans la communauté du renseignement ; auparavant, j'étais pilote d'hélicoptère.

Je commencerai par resituer le commandement cyber (COMCYBER) et par présenter ses enjeux. Puis j'expliquerai en quoi cette LPM répond aux défis de la cyberdéfense.

La fonction cyber est jeune dans l'État : c'est le Livre blanc de 2008 qui a conceptualisé pour la première fois le domaine de la cyberdéfense. L'ANSSI a été créée un an après. Puis le Livre blanc de 2013 a fait de cette fonction une priorité nationale. Plus récemment, en février de cette année, a été publiée une stratégie nationale cyber qui rappelle le niveau de la menace, une menace de plus en plus complexe et qui prend de plus en plus d'ampleurs. Certes, elle ne révolutionne pas l'art de la guerre dans la mesure où ses effets sont assez connus : le recueil d'information et l'espionnage – c'est notre premier souci, en termes de nombre d'attaques –, le sabotage – rappelons-nous ce qui s'est passé en Estonie en 2007 et plus récemment avec TV5 Monde –, des effets enfin de subversion et la désinformation : des événements récents nous ont montré qu'il pouvait y avoir, en pleine période électorale, des effets cyber quasiment existentiels pour nos sociétés. Sans parler de la cybercriminalité, très présente, qui a engendré, selon certains experts, entre 40 et 50 milliards d'euros de bénéfices. C'est enfin une menace en termes de prolifération d'armes : les *Leaks Vault 7* et *Vault 8* ont démontré que les outils d'attaque pouvaient être jetés en pâture dans le domaine public et constituer une menace décuplée contre nos intérêts.

Au-delà de ces menaces, réaffirmées dans la revue stratégique, l'ambition de l'État repose sur un modèle dont les principes sont la séparation d'une part entre la cyberprotection, ce que les Anglo-Saxons appellent l'*information assurance*, et d'autre part le renseignement, et la séparation entre le modèle défensif et le modèle offensif. Ce modèle repose sur quatre acteurs. Le premier est l'ANSSI, qui a la responsabilité de la cyberprotection et la lutte informatique défensive de l'État. Par délégation, j'ai, en tant que deuxième acteur, la responsabilité, au sein du ministère des Armées, de la lutte informatique défensive. Ces deux acteurs s'appuient sur nos services de renseignement, la direction générale de la sécurité extérieure (DGSE) et la direction générale de la sécurité intérieure (DGSI) pour constituer le premier cercle des acteurs de la cyberdéfense.

La mission du COMCYBER repose sur un triptyque. Il exerce tout d'abord une responsabilité normative, à l'image de l'ANSSI, mais restreinte au périmètre du chef d'état-major des armées : autrement dit, je suis chargé de la définition et de la conduite de la politique de sécurité des réseaux placés sous la responsabilité du chef d'état-major des armées. Le COMCYBER exerce ensuite une responsabilité sur toutes les actions, y compris actives, visant à défendre les réseaux de l'ensemble du ministère des Armées. Le troisième pilier enfin, que l'on qualifie d'action numérique, regroupe toutes les actions actives ou offensives visant à mieux soutenir la stratégie de cyberdéfense du ministère, dans le seul champ militaire. Parallèlement, le COMCYBER a une responsabilité de mise en cohérence des politiques de ressources humaines et d'animation de la réserve cyber – j'y reviendrai.

Le premier défi assigné au COMCYBER, mis en place le 1er septembre après du chef d'état-major des armées et comme conseiller du ministre, est un défi d'organisation qui tient tout d'abord à la nécessité de fédérer toutes les chaînes de lutte informatique défensive du ministère des Armées, qu'elles relèvent des armées, du commissariat ou du service de santé des armées, et de les renforcer par une gouvernance centralisée. Il s'agit de s'assurer que tous ces réseaux sont supervisés et parfaitement coordonnés : un incident chez l'un doit pouvoir être partagé chez l'autre. Ce premier défi consiste donc à mettre en place un système tout à la fois fédéré, centralisé et rationalisé. On prévoit de regrouper autour de Paris et Rennes les deux pôles qui constitueront la fonction COMCYBER.

Le deuxième défi est celui de l'adaptation. Une adaptation à l'innovation tout d'abord, car nous sommes dans un monde en constante évolution : on ne peut imaginer des équipements de détection qui ne soient pas modernisés quasiment tous les jours. Ce défi concerne à la fois les processus d'achat, d'homologation et d'intégration de ces équipements dans les structures opérationnelles que je dirige. Une adaptation de l'expertise ensuite, car on est passé, en moins de dix ans, d'une expertise « systèmes d'information » à une expertise cyber. Or le métier de la cyber n'a rien à voir avec celui des systèmes d'information. C'est une fonction qui mêle expertise technique, expertise technologique et capacité analytique pour enquêter sur les réseaux. On est en train de constituer de nouveaux métiers, confiés à une nouvelle population.

Troisième défi, celui du partenariat. De même que pour le contre-terrorisme, on ne peut pas perdre de temps en matière de cyberdéfense. Face à un problème de sécurité collective auquel on ne peut répondre seul, c'est d'abord au sein de l'Union européenne qu'il nous faut essayer d'identifier les pays ayant atteint un niveau de maturité opérationnelle et technique nous permettant d'échanger de la donnée, de prévenir les attaques et de les traiter ensemble ; puis, en dehors de l'Union européenne, nous essayons de voir avec quels autres pays nous pouvons partager la prise en charge de cette cyberdéfense.

Dans la LPM, plusieurs grands axes d'efforts concentrent les ressources qui me sont allouées.

Le premier axe consiste à renforcer nos capacités de détection et d'attribution des attaques. Il s'agit, en d'autres termes, de faire en sorte que nous puissions à la fois concentrer et renforcer nos capacités d'audit des systèmes d'information au profit des armées, des services et des autres réseaux du ministère des Armées. Cette fonction étant actuellement sous-calibrée par rapport à l'ampleur de la demande, ces capacités d'audit seront concentrées au sein d'une structure spécialisée, le CASSI, qui dépend fonctionnellement du COMCYBER.

Le deuxième effort consistera, avec la direction générale de l'armement (DGA), à mieux intégrer le COMCYBER dans l'analyse du risque, tout au long du processus de construction mais aussi de la durée de vie de nos équipements et systèmes d'armes.

Le troisième effort vise à renforcer les capacités de détection qui sont au cœur de la mission du COMCYBER. Il s'agira, d'une part, de renforcer la supervision de l'ensemble des chaînes de détection, assurée par le Centre d'analyse de lutte informatique défensive (CALID) – structure qui est fonctionnellement rattachée au COMCYBER et qui est co-localisée avec l'ANSSI. Cette co-localisation est évidemment essentielle à l'échange d'informations entre l'ANSSI et le COMCYBER. Le CALID verra ses effectifs pratiquement doubler au cours de la LPM. Il s'agira, d'autre part, de se doter de moyens de détection des attaques sur les réseaux du ministère qui en sont pour l'heure dépourvus.

Enfin, le quatrième effort visera à une plus grande réactivité et à une plus grande coordination en cas de crise, conformément aux préconisations de la revue stratégique cyber. Il s'agira de faire en sorte que le COMCYBER puisse, à travers son centre opérationnel, proposer une capacité de coordination des incidents « H 24 », ce qui n'est pas le cas aujourd'hui. La faculté d'intervenir en vingt-quatre heures nécessitant de la ressource, nous ferons en sorte d'avoir cette capacité à coordonner les incidents en temps réel, quelle que soit la posture des armées et du ministère des Armées. Un effort connexe, en matière de réactivité, visera à continuer de nous doter de nos capacités d'action numérique offensives pour être en mesure de mieux attribuer les attaques et faire en sorte de mieux intégrer l'action cyber dans la manœuvre conventionnelle des armées.

**M. Bastien Lachaud.** Mon général, la LPM prévoit une hausse des effectifs, notamment cyber, mais comme dans les autres domaines, un tiers de ces recrutements aura lieu d'ici à 2023 et deux tiers après cette date. Avez-vous une vision plus précise de l'échelonnement dans le temps des recrutements cyber ?

Plusieurs services au sein de notre défense ont des besoins en recrutement cyber, qu'il s'agisse de l'ANSSI, du COMCYBER, de la DGSE ou de la direction du renseignement et de la sécurité de défense (DRSD). Avez-vous une vision plus précise des affectations au sein de ces différents services ?

Enfin, on constate une pénurie de main-d'œuvre dans ce secteur. Comment réussirez-vous à recruter l'ensemble des personnels correspondants aux postes créés ? Comment allez-vous vous coordonner avec les autres services pour éviter toute concurrence entre vous en matière de recrutement ? Comment comptez-vous faire pour pérenniser ces postes et garder vos recrues le plus longtemps possible ?

**M. Thomas Gassilloud.** Quelle est la doctrine du COMCYBER en matière d'intervention sur des théâtres d'opération ? On sait notamment que les opérations aériennes sont commandées depuis Lyon-Mont Verdun. En est-il de même pour les opérations cyber ?

D'autre part, l'article 19 de la LPM autorise les opérateurs de communications électroniques, pour les besoins de la défense et de la sécurité des systèmes d'information, à mettre en place des dispositifs permettant, à partir de marqueurs techniques, de détecter les événements susceptibles d'affecter la sécurité des systèmes d'information de leurs abonnés. Quel type d'événements pourront-ils contrôler ? Pourriez-vous nous en dire plus sur ces dispositifs ?

**Mme Marianne Dubois.** En septembre 2017, le lycée militaire de Saint-Cyr a ouvert un BTS de cyberdéfense. Ce BTS est unique dans son secteur et offre une trentaine de places. Cela est-il suffisant, compte tenu de la montée en puissance attendue de ce secteur ?

**M. M'jid El Guerrab.** Les systèmes d'information liés aux élections sont particulièrement pris comme cibles. Ainsi, le 16 février dernier, la justice américaine a inculpé treize ressortissants russes, accusés d'une possible collusion entre l'équipe de campagne de Donald Trump et la Russie en vue d'influer sur la campagne présidentielle américaine. En France, en avril 2017, la messagerie des membres de l'équipe de campagne d'En Marche a fait l'objet d'une attaque qui a conduit à la publication de ce qu'on a appelé « Macron Leaks », à quelques heures de la fin de la période de campagne. Face aux menaces pesant sur nos élections, le Gouvernement a décidé en mars 2017 de ne pas organiser de vote électronique pour les élections législatives de juin pour les Français résidant à l'étranger, ce qui a entraîné une forte baisse de participation. Qu'est-il prévu pour que l'objectif de mise en place d'un système de vote en ligne parfaitement sécurisé d'ici à 2020 soit atteint ?

**M. Olivier Gaillard, rapporteur pour avis de la commission des Finances.** Ma première question a déjà été posée : par quels moyens financiers comptez-vous fidéliser vos nouvelles recrues ? Plus généralement, où en sommes-nous par rapport à nos voisins européens dans le domaine cyber ?

**M. Jean-François Eliaou, rapporteur pour avis de la commission des Lois.** Mon général, pourriez-vous revenir sur les prérogatives, définies aux articles 19 et 20 de la LPM, que pourra exercer l'ANSSI pour prévenir certaines menaces, sous le contrôle de l'Autorité de régulation des communications électroniques et des postes (ARCEP) ?

Quel sera le profil des personnes que vous comptez recruter ? S'agira-t-il *a priori* de contractuels, sachant que ces technologies sont extrêmement innovantes ? Quel sera leur âge moyen ? Qu'en sera-t-il de leur reconversion dans le civil ?

**Général Olivier Bonnet de Paillerets.** Je commencerai par répondre à vos questions relatives aux ressources humaines.

Pour ce qui est du recrutement, nous sommes en train de constituer une famille de métiers à part entière autour des acteurs de la chaîne cyber des armées – la DGSE, la DGSI, l'ANSSI et le COMCYBER. C'est bien dans cet écosystème qu'il va falloir, à un moment donné, créer des filières pour professionnaliser l'ensemble de la communauté. Plus on crée une communauté, plus on est capable de mener une politique commune de gestion de ressources humaines. Guillaume Poupard et moi-même sommes donc en train de préparer, pour les ressources militaires, les conditions d'un parcours dans les affectations à l'ANSSI et au COMCYBER.

Ensuite, quand on veut recruter une population, on doit réfléchir à sa sociologie. La question du niveau de contractualisation va effectivement commencer à se poser. Ce niveau est très faible actuellement, ce qui n'est pas tenable pour les raisons que vous citiez : ce sont des expertises qui vont finir par se dévaloriser et on a besoin de réoxygéner une partie de l'organisation. Il va donc falloir accepter l'idée d'augmenter la capacité et le niveau de contractualisation au sein de cette communauté.

Vous avez évoqué un déficit de personnel à recruter ; en pratique, aujourd'hui, je suis, au contraire, assez surpris de rencontrer si peu de difficultés de recrutement : nous avons affaire à une génération de jeunes qui ont très envie de servir une fonction régalienne de l'État. Ces jeunes viennent suffisamment en nombre pour répondre à nos besoins. Je parle pour le COMCYBER, mais je suis persuadé que les autres acteurs de la cyberdéfense vous diront la même chose. Cela étant, cette expertise va rapidement être mise en concurrence avec l'extérieur : nous arrivons à recruter, encore faudra-t-il savoir les retenir. Il nous faudra faire en sorte d'adapter nos formules de contractualisation pour maintenir ces jeunes dans nos structures étatiques, le temps qu'ils puissent servir l'État autant que nécessaire, et pour ne les voir partir que lorsque notre organisation pourra se le permettre.

Le volume des formations n'est pas suffisant. Dans mon ancien emploi je me suis fait l'avocat de la création de plus de formations en BTS. Dans la mesure où le cyber est une fonction qui est en train de s'organiser, nous avons besoin de bac + 2 qui se forment chez nous, au contact du métier, afin de devenir opérationnels et à notre main. Il faut multiplier ces cursus car c'est dans cette population que je trouverai une ressource humaine experte, à même d'être efficace dans mes structures opérationnelles.

Au-delà de la formation *ab initio*, le deuxième défi est celui de la formation continue. C'est un réel challenge. Le cyber va très vite ; l'internet modifie ses formats, ses applications tous les jours. Nous avons donc besoin d'une formation continue très robuste et très liée à ce qui se passe dans le monde civil. Nous avons sans doute intérêt à réfléchir à des partenariats public-privé afin de proposer des formations continues à nos opérateurs.

Pour ce qui est de la répartition des effectifs, sur les 1 100 combattants cyber qui sont prévus dans le cadre de la prochaine LPM, un peu plus de 500 relèvent du « grand employeur CEMA » et seront donc directement placés sous l'autorité du COMCYBER. La DGA et les services de renseignement recevront leur quote-part, étant entendu qu'il ne faut pas négliger la DGA qui constitue l'ingénierie de la cyberdéfense au profit des armées.

Pour le grand employeur CEMA, le calendrier prévoit 320 recrutements jusqu'en 2023 et le complément est prévu pour 2025. Cette montée en puissance correspond à ma capacité de recrutement. Je n'ai donc pas de souci à cet égard pour les années à venir, en tout cas pour ce qui concerne le COMCYBER.

Comment utiliser l'action cyber, en parallèle ou en combinaison, dans la manœuvre conventionnelle ? Il s'agit, vous l'avez compris, d'intégrer une nouvelle capacité dans la planification et la conduite des opérations. C'est une question de gouvernance opérationnelle : compte tenu de la nécessité à la fois de protéger cette capacité et d'en maîtriser le risque, il appartient au COMCYBER, placé sous la responsabilité du chef d'état-major des armées, de prendre la décision ou non d'engager ces moyens. Quand un état-major est engagé à l'extérieur, au plus près des combats et de la réalité opérationnelle, toute la question est d'être à même d'établir un dialogue étroit avec le commandement de théâtre qui voudra, ou non, lancer des opérations numériques ; le risque sera évalué par le COMCYBER et ce sera au chef d'état-major des armées, *in fine*, de décider d'engager ou non ces capacités.

Je reviens – veuillez excuser cet esprit d'escalier – sur les ressources humaines et plus précisément sur la question de la réserve. Cette population, j'en suis convaincu, doit être véritablement assimilée à une population active, et pour bien des raisons : non seulement nous

avons énormément de volontaires au titre de la réserve citoyenne, mais, et c'est une autre bonne surprise, ils ont un niveau d'expertise comme je n'en aurai peut-être jamais au COMCYBER. La réserve est donc un enjeu très important pour nous : il faut en améliorer la gouvernance, qui n'est pas encore suffisamment bien assise. La réserve est partie intégrante de la réflexion sur la politique de ressources humaine du COMCYBER.

Qu'en est-il de la cyberdéfense au sein de l'Union européenne ? Prenons – pas tout à fait au hasard – le cas de l'Allemagne qui a décidé de créer un commandement cyber, en fait une sixième armée de 15 000 hommes. Le spectre des missions du commandement cyber allemand n'est pas le même que le COMCYBER : nos voisins y ont intégré l'imagerie satellitaire, le renseignement tactique et une bonne partie de ce qu'on appelle les systèmes d'information opérationnels. La montée en puissance de cette structure, prévue sur trois ans, s'inscrit dans le contexte d'une réforme très profonde des forces allemandes qui s'est faite quelque peu dans la douleur, dont le but est d'organiser une armée à part entière. Les effectifs et moyens sont actuellement renforcés, nos amis allemands ont beaucoup investi dans cette armée cyber et développé de nombreux concepts, si bien qu'il ne fait aucun doute qu'ils deviendront, dans les années 2018-2020, au sein de l'Union européenne, un partenaire de premier plan en matière de cyberdéfense.

Quant aux Britanniques, ils disposent sans doute de l'organisation la plus mature car ils ont commencé à la développer avant nous. Ils ont organisé une interaction de proximité entre les armées, le monde du renseignement et leur ANSSI qui est une émanation du *Government Communications Headquarter* (GCHQ). Nous avions, encore il y a cinq ou dix ans, du retard par rapport à eux, mais nous le rattrapons petit à petit pour, dans les années à venir, les égaler en matière de maturité opérationnelle et organisationnelle. L'un des défis de la Revue stratégique de cyberdéfense a précisément été l'accélération de cette maturation.

Peu d'autres pays de l'Union européenne ont pris la décision de créer un COMCYBER à la mode allemande ou selon le modèle français, plus flexible. Mais ils y viennent : l'Estonie est en train de créer son COMCYBER, l'Espagne se pose la question… Bref, un certain nombre de pays de l'Union européenne gagnent en maturité conceptuelle et devraient, marche après marche, parvenir à se doter d'organisations de cyberdéfense, pour peu qu'ils réalisent les investissements nécessaires.

En ce qui concerne la question sur l'ARCEP comme organisme de contrôle, je me permets de vous renvoyer vers l'ANSSI. Je ne suis pas directement concerné par l'article 19 du projet de LPM, à ceci près que, évidemment, si l'ANSSI active ses capacités de détection en cas d'attaque pouvant concerner le ministère des Armées, j'ai besoin, pour en mesurer l'ampleur, de disposer des informations nécessaires pour les consolider, les corroborer.

De même, la protection et de la pérennisation du vote est de la responsabilité de l'ANSSI et non du COMCYBER. Le ministère des Armées, je le rappelle, mène des actions de protection uniquement sur ses propres réseaux, par délégation de l'ANSSI. Les actions numériques qu'il mène accompagnent l'engagement des armées à l'extérieur du territoire national.

**M. le président.** Pour obtenir des réponses du représentant de l'ANSSI, mes chers collègues, il vous faudra revenir le jeudi 8 mars…

**M. Philippe Michel-Kleisbauer.** Mon général, compte tenu de ce que vous venez d'expliquer sur les puissances qui arrivent à maturité en matière de cyberdéfense et compte tenu du risque ultime que présentent ces cybercapacités, devons-nous réserver les technologies et les techniques à un nombre limité de puissances ? Devons-nous dénier aux autres le droit d'y accéder ?

**Mme Séverine Gipson.** Général, la revue stratégique souligne la réalité et la permanence de la menace cybernétique. Dans le cadre de la LPM, le ministère des Armées considère comme axe prioritaire le dispositif qui garantira son propre fonctionnement et assurera la continuité des grandes fonctions vitales de la nation.

L'article 21 du projet de LPM ajoute les actions numériques à la liste des opérations mobilisant des capacités militaires au cours desquelles la responsabilité pénale du militaire ne peut pas être engagée. Au titre des critères pour lesquels l'excuse pénale pourra être accordée, il est indiqué que « les actions principales devront s'exercer en dehors du territoire national ». Cela signifie-t-il que d'autres actions secondaires pourront être menées à partir du territoire national ? Avez-vous une idée de la façon dont s'opère cette distinction ?

**M. Charles de la Verpillière.** Mon général, pour autant que je connaisse le cyber – c'est-à-dire très peu –, je sais qu'il y a, en la matière, des acteurs étatiques ou para-étatiques et, à l'autre bout du spectre, des acteurs criminels ; et puis il y a aussi des acteurs privés, d'une puissance extraordinaire, que l'on appelle familièrement les GAFA (Google, Apple, Facebook, Amazon), ces grands groupes américains qui traitent des milliards de données. Du point de vue de la cyberdéfense française, considérez-vous les GAFA comme des alliés, des adversaires ou bien des neutres, pour reprendre des termes militaires ?

**Mme Aude Bono-Vandorme.** Devons-nous déduire de l'article 21 du projet de LPM que les personnels civils de la DGA mis à votre disposition ne pourront pas bénéficier de l'excuse pénale ? Il est par ailleurs prévu que cette disposition ne s'applique qu'à des opérations menées hors du territoire national. L'existence d'une dualité de régime entre les OPINT et les OPEX vous paraît-elle pertinente dans le domaine cybernétique ?

**M. Louis Aliot.** Comment jongle-t-on avec ceux qui, d'un côté, sont nos alliés, en particulier aux pays de l'Organisation du traité de l'Atlantique nord (OTAN), mais qui, de l'autre, sont des concurrents, notamment dans l'industrie de la défense, et qui ont pratiqué une forme de nouvel espionnage à nos dépens, comme l'ont révélé plusieurs scandales comme celui de WikiLeaks, ou écouté des conversations par exemple sur le Rafale alors qu'ils nous fournissent des équipements que nous ne fabriquons pas ? Comment dans ces conditions sécuriser nos systèmes ?

**M. Jean-Marie Sermier.** L'informatique et le numérique sont des armes puissantes. Vous avez légitimement évoqué la lutte informatique défensive ou une meilleure détection des attaques. Le projet de LPM prévoit une montée en puissance de notre capacité de cyberdéfense, mais pouvez-vous nous parler d'une éventuelle montée en puissance de notre capacité de cyberattaque ?

**Général Olivier Bonnet de Paillerets.** J'ai soutenu avec force la disposition qui figure aujourd'hui à l'article 21 du projet de LPM parce que je me sens responsable des personnels qui travaillent sous mon commandement. Or je n'étais pas certain que, dans le cadre d'actions numériques que je leur demandais d'exécuter, ils ne fassent pas un jour l'objet

d'une procédure judiciaire – les opérations en question ayant évidemment été validées et les procédures respectées. Je me suis appuyé sur des juristes qui m'ont conseillé de défendre ce dispositif. Peut-être le mot « action » n'est-il pas clair, car c'est surtout de l'effet qu'il s'agit. Les actions cyber conduites au titre du COMCYBER ont un effet en dehors du territoire national. Je ne mène pas d'action dont les effets se produiraient sur le territoire national. Sur ce dernier, je ne m'occupe que de la protection des réseaux du ministère des Armées. Les actions numériques que je conduis le sont, je le répète, à l'extérieur du territoire national, sur un réseau, un groupe de personnes ; et si, par un effet de bord, il y a un risque de judiciarisation, je veux être sûr que l'opérateur du COMCYBER soit pénalement non responsable.

Et ce sont bien les militaires qui mènent des opérations cyber qui doivent bénéficier de ce dispositif. Les civils de la DGA n'entrent pas dans cette catégorie. L'excuse pénale a pour but de garantir la protection de ceux qui sont dans l'action car, vous avez raison, la distinction entre OPINT et OPEX n'a pas grand sens en matière cyber, si ce n'est au regard des limites du mandat du COMCYBER, appelé à engager des effets sur les théâtres où les armées françaises sont engagées.

Faut-il réserver à certains pays la technologie ou non ? À mon sens, le champ de la souveraineté est en train de se déplacer : il faut essayer de rechercher, avec certains pays de confiance et même de grande confiance – et en premier lieu des pays européens –, une convergence entre nos systèmes de détection. Je ne vois pas pourquoi nous ne serions pas capables de nous allier avec les entreprises de ces pays afin de fabriquer des produits qui rendent nos systèmes de cyberdéfense interopérables. Encore une fois, je suis convaincu qu'il s'agit d'un problème de sécurité collective : si l'Allemagne est attaquée, elle doit pouvoir me transmettre en temps réel des données qui me permettront de m'assurer que la France ne l'est pas – pour ce qui concerne le champ militaire en tout cas. Je ne sais pas s'il faut « réserver » des technologies ; en tout cas, je crois qu'il faut faire en sorte que des équipements et des technologies soient mutualisés avec certains pays à même de consolider une communauté d'intérêt sur ce problème de sécurité.

Dans le même ordre d'idées, qui est allié, qui est concurrent ? Cela suppose au préalable de résoudre le problème de la souveraineté. La France et l'Union européenne devront identifier les équipements et les technologies souverains – la revue évoque à cet égard la détection, le chiffrement, les radios, l'intelligence artificielle… On n'a pas encore créé les conditions de cet environnement mais il faut y arriver ; en attendant, c'est une question de gestion de risque : pour tout ce dont sont pourvus les équipements les plus précieux, on doit être à un niveau de confiance, vis-à-vis de l'entreprise ou du pays, qui rende le risque assumable. C'est la seule réponse que nous puissions donner : les révélations de Snowden ne m'ont pas échappé, celles de WikiLeaks non plus avec en particulier les documents *Vault 7* et *Vault 8*. Nous ne sommes pas dans un monde parfait et notre responsabilité est d'admettre que nous ne pouvons que nous inscrire dans le cadre d'une gouvernance du risque tant que nous n'avons pas d'autres solutions.

Les GAFA sont-ils nos alliés, des adversaires ou bien sont-ils neutres ? La réponse est dans la question : un peu des trois… Là encore, les représentants de l'ANSSI seront bien plus précis que moi. Je vais néanmoins tâcher de vous éclairer en vous donnant un exemple. Le COMCYBER, dans ses actions numériques en soutien de l'engagement militaire, par exemple au Levant, surveille la propagande des djihadistes et la combat. Quand un contenu de

cette propagande, en français, va toucher un public français, je le communique au ministère de l'Intérieur et je vérifie avec les responsables de certains des GAFA qu'ils ont bien pris en compte le fait qu'il va falloir retirer ce contenu de la Toile. Nous sommes passés en quelques mois d'une situation où nous n'avions pas de réponse de leur part, à une situation où les taux de retrait sont de 50 à 80 %. J'ai donc réussi, dans le champ opérationnel, à engager un dialogue avec les GAFA et, par le biais du ministère de l'Intérieur, à les sensibiliser un peu plus sur leurs responsabilités. Reste que nous nous trouvons ici dans un contexte d'omnipotence que nous ne pouvons que subir ; le jour où nous serons capables de rééquilibrer les choses au sein de l'Union européenne, tout le monde ne s'en portera que mieux.

Je suis désolé de ne pouvoir répondre à la question portant sur les moyens offensifs. Tout ce que je puis dire est qu'il est illusoire de croire que l'un pourrait aller sans l'autre, qu'on pourrait renforcer l'un sans renforcer l'autre : on ne peut pas bien se défendre si l'on n'a pas la capacité de neutraliser les effets d'une attaque, si l'on n'est pas capable d'engager des moyens actifs. Permettez-moi d'en rester à cette modeste généralité…

**M. Jean-Michel Jacques.** Dès lors que l'armée française intervient sur le territoire national, par exemple avec l'opération Sentinelle, la notion de projection semble toute relative. N'en est-il pas de même s'agissant de la séparation entre la cyberdéfense, qui relève de la défense nationale, et la cybersécurité qui relève de l'ANSSI ? N'aurait-on pas intérêt à tout fusionner pour organiser une défense cyber à la fois intérieure et extérieure ?

Votre niveau d'équipement vous paraît-il convenable pour remplir vos missions ? Les procédures d'acquisition actuelles sont-elles suffisamment fluides ? Vous permettent-elles d'acquérir les matériels dont vous avez besoin et de les remplacer au gré des évolutions technologiques incessantes, ce qui doit poser un certain nombre de problèmes ?

**Mme Laurence Trastour-Isnart.** Le cyberespace, ouvert à tous, évolue en permanence, et nous sommes tous sur les réseaux au quotidien. Comment assurer la cybersécurité au sein de la défense nationale ? Quelles règles internes permettent d'éviter que l'utilisateur lambda au sein de la défense communique des informations par l'intermédiaire des réseaux ? Des règles particulières ont-elles été mises en place en interne ?

**M. Christophe Lejeune.** Nous avons tous en tête des images des défilés militaires sur la place Rouge ou à Pyongyang qui donnent à voir la défense d'un pays. Comment visualiser la cyberdéfense ? Quelle peut être sa portée diplomatique ?

**Mme Josy Poueyto.** La revue stratégique contient des recommandations prioritaires s'agissant en particulier de la consolidation de l'organisation de cyberdéfense française avec la mise en place de quatre chaînes opérationnelles : « protection », « action militaire », « renseignement », et « investigation judiciaire ». Comment s'articulent-elles ?

**M. Thibault Bazin.** Mon général, la LPM aurait pu prévoir un volet contenant un arsenal d'outils juridiques que vous auriez utilisés comme autant d'armes. En particulier, ne devrions-nous pas changer de doctrine ? Notre stratégie est très différente de celle de l'Allemagne. Notre approche est transversale alors que les Allemands mettent en place une véritable armée cyber. L'option française a-t-elle donné lieu à un débat puis à un arbitrage ?

**Général Olivier Bonnet de Paillerets.** M. Jean-Michel Jacques a relevé la continuité du rôle des armées à l'extérieur et à l'intérieur avec l'opération Sentinelle. Je ne puis que répéter que si le COMCYBER a bien la responsabilité de défendre les réseaux informatique et de télécommunication utilisés par Sentinelle, il n'a aucune responsabilité en matière d'action cyber sur le territoire national autre que ce qui relève de la défense.

Je vous confirme qu'il n'y a pas de continuité en matière d'action cyber : seuls les services de police et de renseignement sont autorisés par la loi à mettre en œuvre des techniques de renseignement sur le territoire national – y compris sur la base d'actions informatiques. Le COMCYBER n'y est pas autorisé. Je ne mène pas d'actions numériques sur le territoire national ; ma responsabilité concerne l'extérieur et les théâtres en soutien.

En matière d'équipements, un double effort doit être engagé à travers la LPM. Le premier concerne l'industrialisation des moyens de détection et de supervision. Ce changement d'échelle constitue un défi. Je dois m'assurer que des sondes dans l'ensemble du réseau des armées me permettent de centraliser, au niveau du CALID, une hypervision des informations qui remontent, et une coordination des éventuels incidents. Mon premier défi est donc celui de l'industrialisation de toute la chaîne de détection du ministère des Armées, y compris en intégrant dans les années à venir tout ce que l'intelligence artificielle générera en termes d'automatisation, d'enrichissement, de moyens de détection et de supervision. En l'état actuel des choses, peut-on dire que tout est parfait ? Je n'irai pas jusque-là, mais le ministère des Armées dispose bel et bien de moyens de détection et d'hypervision. Des investissements sérieux sont toutefois nécessaires pour assurer le passage à l'échelle appropriée, ce qui nécessitera une importante approche programmatique avec la DGA.

Le second effort concerne la capacité à intégrer des équipements qui répondent aux besoins opérationnels immédiats des structures opérationnelles, qu'il s'agisse du CALID ou du CO CYBER. Nous avons pris la décision, avec la DGA, de mettre en place des circuits courts d'achat en lançant des « défis » aux entreprises françaises. Nous leur disons par exemple : « Dans les six mois, j'ai besoin d'une capacité d'analyse de données projetable pour me moderniser et accompagner les forces à l'extérieur du territoire. » À elles de me proposer un produit dans les six mois. S'il me convient, nous passons à l'échelle industrielle. Nous mettons en place des systèmes qui nous permettront de disposer d'équipements sur des temps courts, car le temps court correspond aux réalités de l'innovation et de l'accélération technologique liée à l'internet.

Comment puis-je m'assurer que les militaires et les civils qui travaillent pour nous respectent les règles de confidentialité ? Tous ceux qui rejoignent le COMCYBER font évidemment l'objet d'une enquête qui permet de leur attribuer un niveau d'habilitation *ad hoc*. Par ailleurs, je mets actuellement en place une charte de déontologie qui, au-delà des aspects réglementaires, vise à créer une identité commune autour de valeurs professionnelles, mais également de la notion de responsabilité. Ces chartes de déontologie permettent de marquer les esprits et d'organiser collectivement la responsabilité des actions individuelles.

Existe-t-il un lien entre le cyber et la diplomatie ? D'une certaine manière, le cyber change le statut des États, parce que ceux qui se numérisent sont les plus en pointe en matière de cyberdéfense, ce qui signifie qu'ils disposent aussi de capacités cyber offensives. Ce statut ouvre la possibilité de partenariats et d'échanges et permet d'accéder à des responsabilités politiques nouvelles, y compris dans les chaînes diplomatiques. Pour des raisons liées à

l'économie et à la sécurité collective, la cyber est aujourd'hui devenue un vecteur de rapprochement à part entière. Elle constitue bien une dimension de notre diplomatie.

Il est un peu difficile de comparer les ambitions des armées françaises et allemandes en matière de cyberdéfense. L'armée française est dans les opérations au quotidien. Nous avons décidé d'une gestion plutôt transversale de la responsabilité cyber, ce qui m'évite de devoir gérer chaque jour des questions organiques. Je peux me concentrer sur ma responsabilité opérationnelle et fonctionnelle. J'ai l'autorité opérationnelle sur les structures (CALID, CASSI…) et d'autres s'occupent de leur fonctionnement. Je ne vois aucun problème à ne pas disposer de rattachements organiques aussi imposants que ceux décidés en Allemagne. Tout l'enjeu est de parvenir à identifier et faire accepter des mécanismes de gouvernance efficaces: comme toute nouvelle capacité, elle doit être comprise et accompagnée. Le défi que j'ai à relever, c'est de faire monter en puissance la culture collective des armées dans ce domaine. J'estime aujourd'hui que la fonction transverse qui est la mienne me permet d'exercer mes missions. Cela relève de l'exercice de ma responsabilité et de mon *leadership*, ainsi que de ceux de mes adjoints : à nous de faire en sorte que cette fonction transverse soit acceptée et apporte de la plus-value au système.

Les quatre chaînes opérationnelles sont articulées autour des quatre acteurs dont je vous ai parlé. Parce que ce modèle a séparé l'offensif, le défensif, l'*information assurance* et le renseignement, la revue stratégique a souhaité mettre en place un système de coordination de l'ensemble acteurs. Ceux-ci participeront non seulement à un comité stratégique qui veillera à la montée en puissance de la communauté cyberdéfense, mais aussi à des centres de coordination des crises cyber (C4) qui permettront d'améliorer le partage de l'analyse de la menace, la coordination et l'organisation d'une réponse en cas de crise. La revue cyber prévoit donc de maintenir le modèle français fondé sur des principes de séparation tout en organisant une coordination aux niveaux politiques, opérationnels et techniques pour veiller à ce que ces quatre piliers fonctionnent ensemble.

La fonction cyber est opérationnelle. Elle est devenue une capacité à part entière ; le ministère des Armées et le chef d'état-major n'ont aucun doute sur ce point., le temps viendra où nous participerons à un défilé du 14 juillet pour montrer que la France est une puissance cyber, et qu'elle l'assume dans le champ militaire.

**M. Patrick Hetzel.** La réserve de cyberdéfense créée en 2016, chargée d'assister l'État et les armées en cas de crise numérique majeure, est placée sous votre autorité. Son périmètre d'intervention vous semble-t-il satisfaisant ? Vous avez parlé d'aller un peu plus loin. Quelles évolutions seraient souhaitables afin d'assurer son efficacité optimale ?

Pouvez-vous nous dire comment le commandement de cyberdéfense coordonne ses actions avec le SGDSN qui a autorité sur l'ANSSI ?

**Mme Patricia Mirallès.** Selon vous, est-il nécessaire de développer des systèmes informatiques d'État afin de préserver l'ensemble de nos données et d'assurer la sécurité du pays ?

Que pensez-vous d'un *Patriot Act* à la française ?

**M. Loïc Kervran.** Vous me pardonnerez de revenir sur la question de l'article 19 de la future LPM. J'ai compris les limites de votre compétence en matière de défense intérieure –

sauf dans le cas où une attaque concernerait les systèmes du ministère des Armées. Le modèle français a en effet la particularité de distinguer le défensif, qui relève de l'ANSSI, de l'offensif qui entre dans votre champ de compétence – et sans doute également dans celui d'autres organes comme la DGSE. Dans ce modèle, n'est-il pas envisagé d'utiliser les informations recueillies par les marqueurs techniques disposés par l'ANSSI ou les opérateurs pour apporter une réponse offensive appropriée en cas d'attaque ? Une démarche de cette nature n'impliquera-t-elle pas une « désanonymisation » des données en question ?

**M. Laurent Furst.** Mon général, j'ai appris que les Français « utilisent », au quotidien, en moyenne, quarante-six ou quarante-sept satellites. Nous avons déjà repéré un objet parfaitement identifié, mais non dénommé, non loin d'un satellite français. Il paraît également que des bâtiments russes auraient été localisés à proximité des câbles sous-marins qui sillonnent la planète pour transporter l'information. Nous avons conscience de la dimension cyber du champ de combat, mais votre métier consiste-t-il aussi à assurer la protection des communications et des données des Français qui passent par les satellites et les câbles sous-marins – qui peuvent du reste appartenir à des entreprises de taille internationale relevant d'un autre pays ? Votre mission s'exerce-t-elle aussi dans les eaux internationales ou dans l'espace ?

**M. Fabien Lainé.** La cybersécurité est un système d'interdépendance qui nécessite d'éviter les maillons faibles et les portes d'entrée qui permettent les attaques. Ce système ne peut donc être efficace que si chacun est sensibilisé à ces exigences. J'ai entendu que vous souhaitiez rédiger une charte de déontologie et de bonnes pratiques, mais pensez-vous que le niveau de formation des personnels civils et militaires du ministère des armées soit aujourd'hui à la hauteur de ces enjeux ?

**M. Philippe Chalumeau.** Avec l'irruption l'intelligence artificielle et l'informatique quantique, nous savons que nous allons vers une révolution exceptionnelle, d'une ampleur comparable à celle que provoqua l'invention de la poudre. Estimez-vous que la LPM vous accompagne et qu'elle apporte une réponse suffisamment calibrée pour faire face aux nouveaux risques ? Selon vous, à partir de quand peut-on attendre leur explosion et leur progression exponentielle ?

**Général Olivier Bonnet de Paillerets.** Peut-être aurais-je dû le préciser, il existe deux réserves de cyberdéfense : la réserve citoyenne de cyberdéfense (RCC), gouvernée par le triptyque gendarmerie-ANSSI-COMCYBER, et la réserve opérationnelle de cyberdéfense, directement placée sous l'autorité du COMCYBER. En tant que responsable de ces deux réserves, je suis confronté à plusieurs enjeux. Tout d'abord, nous sommes en train de réviser en profondeur les missions et la gouvernance de la réserve citoyenne de cyberdéfense. Actuellement, celle-ci est utilisée pour réaliser des actions de sensibilisation à la cyberdéfense et de communication concernant le COMCYBER et les besoins du ministère. Or, pour vous dire les choses franchement, ce n'est pas ainsi que l'on motive des réservistes, qui veulent travailler pour une structure opérationnelle. Il faut donc rapprocher cette réserve des besoins quotidiens du COMCYBER, y compris sur le plan opérationnel. Par ailleurs, si sa gouvernance parisienne a été très bien pensée, ce n'est pas le cas au niveau territorial. Nous avons donc décidé, avec l'ANSSI et la gendarmerie, de créer des gouvernances dans treize régions afin qu'elle s'inscrive davantage dans le tempo des besoins du COMCYBER, de l'ANSSI ou de la gendarmerie. Il s'agit d'une réforme assez lourde.

Vous l'aurez compris, je souhaiterais atténuer la distinction entre les deux réserves. En effet, il ne me paraît pas sain de créer un fonctionnement à deux vitesses, les motivations étant différentes dans chacune des deux réserves. J'ai besoin d'une partie de leur expertise et je ne voudrais pas que des problèmes de statuts ou de dénomination de missions m'interdisent d'utiliser l'une ou l'autre. Nous sommes donc en train de réfléchir aux moyens de créer entre ces deux réserves une interaction afin que le COMCYBER puisse, en définitive, se tourner vers une population globale et faire appel à l'une ou l'autre selon qu'il a besoin du maillage de la réserve citoyenne ou de la réserve opérationnelle de cyberdéfense. Le défi que nous devons relever consiste, encore une fois, à disposer d'une réserve active qui s'inscrive dans le tempo du besoin quotidien des opérations du COMCYBER.

Par ailleurs, la relation entre le COMCYBER et le SGDSN se fait directement avec l'Agence nationale de sécurité des systèmes d'information, à plusieurs niveaux. Tout d'abord, le centre nerveux et opérationnel du COMCYBER est co-localisé avec l'ANSSI. Ma structure, le CALID, qui a pour mission de superviser les réseaux du ministère des Armées, a ainsi directement accès aux informations, aux expertises ou aux formations dont il a besoin. Cette co-localisation crée un terreau très favorable à l'interaction avec l'ANSSI et le SGDSN.

Mais Guillaume Poupard – le directeur général de l'ANSSI, avec qui j'ai une relation très précieuse – et moi-même souhaitons faire en sorte que le champ du partenariat entre le COMCYBER et l'ANSSI ne se limite pas à cette co-localisation : nous voulons pouvoir réfléchir à des politiques de ressources humaines et de formation continue communes ainsi qu'à une mutualisation des équipements. Il s'agit également de mettre en œuvre une politique partenariale pour remédier aux problèmes de symétrie d'organisation auxquels nous sommes constamment confrontés avec les pays étrangers ; de fait, tous les pays n'ont pas une ANSSI et un COMCYBER. Du reste, je rappelle que, si j'ai la responsabilité opérationnelle au regard du CEMA et du ministère des Armées, je suis sous la responsabilité de l'ANSSI pour ce qui touche aux aspects réglementaires et normatifs.

La question du *Patriot Act* ne relève pas du COMCYBER, mais de l'ANSSI… Faut-il des systèmes d'État ? Encore une fois, c'est une question extrêmement lourde. J'en reviens à l'idée de la souveraineté : ne faut-il pas envisager une souveraineté partagée ? Je ne fais là que soulever la question – mais vous aurez compris mon inclination.

À propos de l'article 19, il me semble naturel que l'on renforce les prérogatives de l'ANSSI pour qu'elle puisse mettre en place, dans certaines structures d'intérêt, des systèmes de détection d'attaques qui, directement ou indirectement, vont toucher les intérêts de l'État. Ensuite, il revient à l'ANSSI, qui est au point d'équilibre entre la cyberprotection, le renseignement et l'offensive, de décider ou pas du transfert des marqueurs, par exemple. C'est fondamentalement le SGDSN qui sera à la manœuvre dans ce domaine. Ce que je dis simplement, c'est que, agissant sur délégation de l'ANSSI, il faut que, si cette attaque touche le ministère des Armées, mes chaînes de détection me permettent de la corroborer et de mesurer son amplitude et son agressivité. C'est un environnement sur lequel nous devrons travailler avec l'ANSSI, pour définir un protocole, des règles de bonne conduite, etc.

Je n'exerce pas de responsabilités directes dans la protection des câbles, qu'ils touchent le territoire national ou qu'ils se trouvent dans les eaux territoriales. Quant aux satellites de communication, seuls les satellites militaires relèvent de ma responsabilité ; les satellites civils relèvent de l'ANSSI. Cependant, lorsque les intérêts français sont touchés, le

COMCYBER a le devoir de soutenir ceux qui les défendent dans un champ non militaire et il a la responsabilité de développer des scénarios qui permettent de neutraliser l'agresseur ou de diminuer les effets de son attaque. C'est ainsi que j'interviens, indirectement, en proposant des options de nature militaire au niveau politique.

En ce qui concerne la formation, je reprendrai une des conclusions de la revue stratégique cyber : nous devons former nos concitoyens, dès le plus jeune âge, à la notion de cybersécurité. C'est très bien d'avoir un téléphone portable ou d'être inscrit sur Facebook ; encore faut-il en mesurer les conséquences. Plus tôt nous les sensibiliserons à cette culture et nous les responsabiliserons dans leur utilisation des outils connectés à internet, mieux ce sera. Ce qui est vrai pour nos concitoyens l'est également pour le ministère des Armées mais, même si l'on peut toujours mieux faire, je crois que celui-ci a pris un peu d'avance dans ce domaine. Le véritable enjeu réside plutôt dans l'organisation de la formation continue. Je veux en effet m'assurer que le niveau de professionnalisation des opérateurs du COMCYBER demeure le plus haut possible.

La DGA s'est engagée, il y a quelques années, dans l'expertise de l'intelligence artificielle. Frédéric Valette, l'un des adjoints du DGA, chargé du domaine cyber, avec qui je collabore étroitement, me tient informé de l'évolution des programmes et des investissements réalisés dans ce domaine. Je n'ai donc pas d'inquiétudes : la DGA m'accompagnera dans la mise en place et l'intégration de l'intelligence artificielle. Celle-ci suscite beaucoup d'interrogations, qu'il s'agisse du management de l'information dans les états-majors, de la manière dont le *deep learning* et la robotisation permettront d'améliorer le fonctionnement de la cyberdéfense… L'enjeu pour moi est de faire en sorte que, dans la trajectoire de la LPM, la révision de l'ensemble de l'architecture de détection et de supervision puisse coïncider avec le moment où les techniques liées à l'intelligence artificielle arriveront à maturité : le but, et nous y travaillons avec Frédéric Valette, est d'éviter toute obsolescence dans les programmes que nous avons lancés et de faire en sorte que, dès que la virtualisation et le *deep learning* arriveront à maturité, on puisse les intégrer naturellement dans les architectures en cours d'élaboration.

**M. le président.** Je laisse la parole à Jean-François Eliaou, pour une dernière question, qui sera brève.

**M. Jean-François Eliaou.** Permettez-moi de revenir sur l'article 21, Mon général. Les acteurs du COMCYBER pourraient-ils être confrontés à des problèmes de judiciarisation pénale dans leur activité de protection sur le territoire national ?

**Général Olivier Bonnet de Paillerets.** Je ne vois pas quel scénario pourrait les mettre en danger car, dans le cadre de la détection et de la supervision, nous ne faisons à aucun moment appel à des capacités actives ; nous n'utilisons que des capacités passives qui entrent dans un champ réglementaire qui me semble très bordé. Le COMCYBER et l'ANSSI peuvent, en vertu de l'article 21 de la dernière LPM, neutraliser les effets d'une attaque sur le territoire national par des moyens actifs. Cette possibilité existe, mais elle est parfaitement encadrée.

**M. le président.** Merci pour vos réponses, Mon général.

*La séance est levée à seize heures trente.*

*

* *

**Membres présents ou excusés**

*Présents.* - M. Louis Aliot, M. Pieyre-Alexandre Anglade, M. Thibault Bazin, M. Christophe Blanchet, Mme Aude Bono-Vandorme, M. Jean-Jacques Bridey, Mme Carole Bureau-Bonnard, M. Philippe Chalumeau, Mme Marianne Dubois, M. M'jid El Guerrab, M. Jean-Jacques Ferrara, M. Jean-Marie Fiévet, Mme Pascale Fontenel-Personne, M. Laurent --Michel Jacques, M. Loïc Kervran, Mme Anissa Khedher, M. Bastien Lachaud, M. Fabien Lainé, M. Christophe Lejeune, M. Philippe Michel-Kleisbauer, Mme Patricia Mirallès, Mme Josy Poueyto, Mme Laurence Trastour-Isnart, M. Charles de la Verpillière

*Excusés.* - M. Damien Abad, M. Bruno Nestor Azerot, M. Florian Bachelier, M. Olivier Becht, M. Luc Carvounas, M. André Chassaigne, M. Jean-Pierre Cubertafon, M. Stéphane Demilly, Mme Françoise Dumas, M. Olivier Faure, M. Yannick Favennec Becot, M. Richard Ferrand, M. Marc Fesneau, M. Claude de Ganay, M. Christian Jacob, M. Jean-Christophe Lagarde, M. Jean-Charles Larsonneur, M. Jacques Marilossian, Mme Sereine Mauborgne, M. Gwendal Rouillard, M. François de Rugy, Mme Sabine Thillaye, Mme Alexandra Valetta Ardisson

*Assistaient également à la réunion.* - M. Jean-François Eliaou, M. Olivier Gaillard, M. Patrick Hetzel, M. Jean-Marie Sermier, M. Jean-Luc Warsmann