ASSEMBLÉE NATIONALE

14ème législature

sécurité

Question écrite n° 102215

Texte de la question

M. Lionel Tardy interroge M. le ministre de la défense sur la création d'un futur commandement des opérations cyber, qu'il a annoncée en décembre 2016. Ce « Cybercom » supervisera 2 600 « combattants numériques » d'ici 2019, et sera précédée par une structure préfiguratrice lancée le 1er janvier 2017. Outre les moyens humains, il souhaite connaître les moyens budgétaires prévisionnels alloués, d'une part, à ce commandement, et d'autre part, ceux affectés à la structure préfiguratrice.

Texte de la réponse

Le Livre blanc sur la défense et la sécurité nationale, approuvé par le Président de la République en avril 2013, a élevé la cyberdéfense au rang de priorité nationale. En effet, la part croissante prise par le cyberespace dans nos moyens de défense et notre économie engendre des risques qui peuvent se révéler stratégiques. Aussi, les enjeux de cyberdéfense appellent-ils une mobilisation de toute la communauté nationale afin de constituer les ressources humaines et les compétences dont la Nation a besoin pour innover et se défendre. De nombreuses mesures ont déjà été adoptées pour répondre à ces enjeux. Le Pacte « Défense Cyber », lancé par le ministre de la défense en février 2014, a ainsi permis de mettre en œuvre 50 actions destinées notamment à augmenter le niveau de sécurité des systèmes d'information, à renforcer les moyens de défense et d'intervention du ministère et de ses grands partenaires de confiance et à préparer l'avenir en intensifiant l'effort de recherche technique, académique et opérationnel, tout en soutenant la base industrielle. Par ailleurs, la loi no 2013-1168 du 18 décembre 2013 relative à la programmation militaire (LPM) pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, modifiée par la loi no 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019, dispose que les moyens du ministère de la défense consacrés à la cyberdéfense accéléreront leur montée en puissance avec le recrutement d'au moins 1 000 civils et militaires d'active supplémentaires sur la période 2014-2019. De même, avec près de 440 millions d'euros, la LPM prévoit de multiplier par trois les crédits dédiés au développement et à l'acquisition de nouvelles solutions de cybersécurité sur la période précitée. Il convient d'ajouter qu'à la suite des attentats commis à Paris le 13 novembre 2015, le Président de la République a déclaré, devant le Parlement réuni en Congrès à Versailles, qu'il n'y aurait aucune diminution des effectifs de la défense jusqu'en 2019. En conséquence, lors du conseil de défense et de sécurité nationale du 6 avril 2016, le chef de l'État a décidé que 10 000 postes supplémentaires seraient préservés, permettant un redéploiement des effectifs en vue de satisfaire prioritairement les besoins identifiés des unités opérationnelles et de leurs soutiens, ainsi que dans les secteurs de la cyberdéfense, du renseignement et de la protection du territoire national. Comme le ministre de la défense l'a rappelé à l'occasion de son discours prononcé lors de son déplacement sur le site de la direction générale de l'armement à Bruz, le 12 décembre 2016, les menaces dans le cyberespace sont le fait d'une diversité inédite d'acteurs. Elles recouvrent en outre des réalités profondément asymétriques, dans lesquelles de faibles moyens permettent d'obtenir des effets importants, analogues à ceux d'actions plus conventionnelles, en particulier lorsqu'elles visent des infrastructures civiles critiques, voire des cibles militaires. Ces menaces sont appelées à s'intensifier. Par ailleurs, la fréquence et l'ampleur des attaques dans le cyberespace ne cessent de

croître, tout comme leur sophistication technologique, témoignant ainsi d'une prolifération préoccupante des moyens d'agression. Face à ce constat, le ministre estime que la défense de la France doit s'adapter aux enjeux actuels et futurs du champ de bataille cyber et qu'il est aujourd'hui indispensable de développer une nouvelle doctrine et une stratégie cyber de défense. Cette doctrine de cyberdéfense s'articulera ainsi autour de 4 axes majeurs : missions, coopération internationale, domaine juridique et moyens. Elle nécessite que le ministère de la défense se réorganise en vue de créer une nouvelle composante au sein des armées. Le ministre de la défense a donc décidé la création d'un commandement des opérations cyber (COMCYBER) qui l'assistera en matière de cyberdéfense et sera placé sous la responsabilité directe du chef d'état-major des armées. Un état-major de la cyberdéfense, structure de préfiguration du commandement de la cyberdéfense, a été créé par décision no 1031/DEF/CAB/CMIN du 12 janvier 2017 publiée au Bulletin officiel des armées du 2 février 2017. Cette structure de préfiguration est chargée de la conception, de la définition et de la préparation du futur COMCYBER. Elle sera dissoute à la date d'entrée en vigueur des textes portant création et attributions du COMCYBER et de son état-major. S'agissant des missions du COMCYBER, outre ses responsabilités de cohérence organique du domaine de la cyberdéfense, il assurera 4 fonctions principales : la protection, la défense, l'action numérique et le combat informatique, ainsi que le développement des réserves de cyberdéfense. L'état-major du COMCYBER devra quant à lui notamment être en mesure de protéger les systèmes d'information du ministère de la défense ; de concevoir, planifier, préparer et conduire les opérations militaires dans l'espace numérique ; de contribuer à concevoir et à mettre en œuvre une politique des ressources humaines de cyberdéfense et de coordonner la contribution des armées et organismes interarmées à la politique nationale et internationale de cyberdéfense. Par ailleurs, à l'horizon 2019, le COMCYBER aura autorité sur toutes les unités opérationnelles spécialisées dans la cyberdéfense du ministère, soit 2 600 combattants numériques, auxquels s'ajouteront 600 experts de la DGA. Ces forces seront complétées par 4 400 réservistes de cyberdéfense (4 000 réservistes citoyens et 400 réservistes opérationnels). En matière d'effectifs, il est précisé que cette structure nouvellement instituée englobe la cellule de cyberdéfense de l'état-major des armées ainsi que le commandement de cyberdéfense, organisme interarmées créé par décision du 13 juin 2016. Elle réunit ainsi, dès à présent, 58 militaires et civils. Par la suite, l'effectif du COMCYBER devrait être renforcé pour atteindre environ 110 personnes en 2019. Ces effectifs sont imputés au plan de montée en puissance de la fonction de cyberdéfense décidé lors de l'actualisation de la LPM pour les années 2014 à 2019. A l'instar des ressources humaines, les moyens financiers dont bénéficie la structure de préfiguration, et qui seront accordés à terme au COMCYBER, sont ceux qui avaient été prévus au profit des structures préexistantes. Le financement des activités de cyberdéfense, à l'exception de celles prises en charge pour leurs besoins propres par les armées et organismes interarmées, repose sur les programmes 178 « Préparation et emploi des forces », 144 « Environnement et prospective de la politique de défense » et 146 « Équipement des forces ». L'évolution prévue des ressources financières allouées à la cyberdéfense au titre de la mission « Défense » figure dans le tableau suivant :

Ressources globales (en millions d'euros)						
Années	2017	2018	2019	2020	2021	2022
Mission « Défense »	104,18	118,38	117,05	111,59	111,96	112,47

Ce budget permettra de financer notamment les projets d'étude amont afin de faire progresser la recherche et le développement en matière de cybersécurité, ainsi que les opérations de cyberdéfense du ministère (incluant le développement de capacités et leur emploi), le fonctionnement courant de l'état-major, l'instruction et la formation dans le domaine de la cyberdéfense et l'acquisition de petits équipements spécifiques et de prestations au profit des unités spécialisées de cyberdéfense (centre d'analyse en lutte informatique défensive,

centre d'audits de la sécurité des systèmes d'information). Il pourvoira également au financement des opérations d'armement liées notamment aux capacités de protection de nos systèmes d'information et aux moyens de lutte informatique défensive et d'influence numérique.

Données clés

Auteur : M. Lionel Tardy
Circonscription : Haute-Savoie (2e circonscription) - Les Républicains
Type de question : Question écrite
Numéro de la question : 102215
Rubrique : Défense
Ministère interrogé : Défense
Ministère attributaire : Défense

Date(s) clée(s)

Question publiée au JO le : 31 janvier 2017, page 676
Réponse publiée au JO le : 16 mai 2017, page 3553