ASSEMBLÉE NATIONALE

14ème législature

télécommunications

Question écrite n° 30166

Texte de la question

M. Jean-Louis Bricout attire l'attention de M. le ministre de la défense sur la cyberdéfense. En effet, dans un contexte de maîtrise de la dépense publique et suite au Livre blanc rendu public le 29 avril 2013, il lui demande quelles orientations il compte mettre en oeuvre à propos de ce sujet dont on sait qu'il constitue un enjeu vital.

Texte de la réponse

En mettant l'accent sur la fréquence et l'impact potentiel de la menace que constituent les cyberattaques visant nos systèmes d'information et qui imposent d'augmenter très significativement leur niveau de sécurité et les moyens de leur défense, le Livre blanc sur la défense et la sécurité nationale, paru le 29 avril 2013, confirme l'importance stratégique que revêt le cyberespace et érige la cyberdéfense en priorité nationale. A cet égard, il convient d'observer que des progrès significatifs ont été réalisés depuis le précédent Livre blanc de 2008, avec notamment la création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), la publication d'une stratégie nationale pour la cyberdéfense, la publication d'un concept et d'une doctrine militaires de cyberdéfense et la création d'un commandement opérationnel de cyberdéfense intégré au centre de planification et de conduite des opérations de l'état-major des armées. Cette chaîne de commandement spécifique au cyberespace a été mise en place pour organiser et assurer la défense des systèmes d'information du ministère et des armées (systèmes de communications, systèmes d'armes et systèmes industriels) face aux menaces d'attaques informatiques. Elle a également pour mission de conduire d'éventuelles offensives informatiques en soutien des opérations militaires. Afin de poursuivre et d'encadrer l'ensemble de ses efforts, le ministère de la défense a élaboré un schéma directeur capacitaire de cybersécurité, approuvé en juin 2012. Ce document, servant en ce domaine de base pour l'élaboration de la loi de programmation militaire (LPM) 2014-2019, prévoit des évolutions de doctrine, ainsi qu'un renforcement des moyens humains et techniques dédiés. Parallèlement, d'importants travaux pilotés par la direction générale des systèmes d'information et de communication du ministère ont été lancés en matière de ressources humaines. Par ailleurs, une commission spécialisée dans le domaine de la formation à la cybersécurité a été constituée et la création en Bretagne d'un centre de formation à la cyberdéfense est envisagée. Dans ce contexte, le ministère compte aujourd'hui environ 1 600 personnes investies dans la cyberdéfense dont 1 200 agents travaillent au sein des armées avec 300 d'entre eux en charge des équipements de chiffrement et 900 autres au profit des chaînes de prévention, de protection et de défense des systèmes. Des groupes d'intervention rapide sont susceptibles de se déployer sur tout le territoire national et sur chaque théâtre d'opérations extérieur dans le but de circonscrire une attaque informatique. La future LPM devrait confirmer le plan d'augmentation, à hauteur de 300, des spécialistes de la sécurité informatique des systèmes d'armes et des infrastructures industrielles du ministère. Pour sa part, la direction générale de l'armement (DGA) a considérablement accru son expertise en cybersécurité. Ses effectifs spécialisés ont augmenté de 60 % au cours des trois dernières années et regrouperont environ 400 experts de très haut niveau d'ici à 2017. En outre, dans le cadre de la LPM 2014-2019, les moyens alloués à l'acquisition et au fonctionnement des équipements propres à la cybersécurité devraient connaître une forte progression pour atteindre un montant proche de 360 M€ sur la période considérée. S'agissant des crédits consacrés à la

recherche et au développement, ces derniers devraient tripler et représenter chaque année une somme de 30 M€. Par ailleurs, le ministère vient de créer une réserve citoyenne praticienne de la cyberdéfense, qui réunit déjà plus de 60 réservistes actifs des trois armées et de la gendarmerie nationale, dont la mission couvre la réflexion et la promotion autour de la cyberdéfense. Des groupes de travail ont été constitués et rassemblent à la fois des réservistes citoyens (ingénieurs, juristes, magistrats, managers, fonctionnaires, chercheurs, étudiants...) et des membres de la société civile non réservistes. Ce réseau, composé de profils très variés permettant d'apporter un regard croisé sur la cyberdéfense, mène des travaux en commun avec l'ANSSI, la DGA et la direction générale de la gendarmerie nationale. A court terme, il est prévu d'étendre son influence, en province, à de nouveaux acteurs de la société civile comme les petites et moyennes entreprises et industries. Dans le cadre de la réserve militaire opérationnelle, quelques postes de spécialistes en cyberdéfense ont également été ouverts et ont d'ores et déjà été honorés. Enfin, les premiers retours d'expérience face à des attaques informatiques de grande ampleur montrent qu'après avoir identifié et caractérisé une offensive, il convient de remettre à niveau ou de redéployer le système d'information de l'organisme attaqué. Ces opérations peuvent prendre la forme d'une intervention sur plusieurs dizaines de milliers de postes informatiques devant nécessairement être réalisée dans des délais réduits. Une réflexion a donc été engagée afin de parvenir à mobiliser rapidement un personnel très nombreux compétent et habilité pour soutenir l'État dans la gestion d'une crise de cette nature.

Données clés

Auteur : M. Jean-Louis Bricout
Circonscription : Aisne (3e circonscription) - Socialiste, écologiste et républicain
Type de question : Question écrite
Numéro de la question : 30166
Rubrique : Défense
Ministère interrogé : Défense
Ministère attributaire : Défense

Date(s) clée(s)

Question publiée au JO le : 25 juin 2013, page 6558
Réponse publiée au JO le : 6 août 2013, page 8447