ASSEMBLÉE NATIONALE

14ème legislature

Question N° : 1956	De **M. Patrick Hetzel** (Union pour un Mouvement Populaire - Bas-Rhin)	**Question écrite**

Ministère interrogé > Défense	**Ministère attributaire** > Défense

Rubrique >défense	**Tête d'analyse** >télécommunications	**Analyse** > cyberdéfense. rapport. propositions.

Question publiée au JO le : **31/07/2012**
Réponse publiée au JO le : **30/10/2012** page : **6126**

Texte de la question

M. Patrick Hetzel souhaite interroger M. le ministre de la défense à la suite de la remise du rapport de M. Jean-Marie Bockel au Sénat sur la cyberdéfense. Cinquante propositions ont été développées. Il souhaite savoir quelle suite va être donnée à ces conclusions tout particulièrement dans le domaine de la défense qui est fortement concerné.

Texte de la réponse

Le Livre blanc sur la défense et la sécurité nationale de 2008 a identifié différents axes d'efforts destinés à structurer le dispositif national de cyberdéfense et a donné l'impulsion au développement des capacités de veille et de protection. Le rapport d'information du Sénat sur la cyberdéfense, publié 18 juillet 2012, a établi cinquante recommandations, rassemblées en dix priorités. Ces orientations, qui constituent des axes de réflexion pour l'élaboration du nouveau Livre blanc sur la défense et la sécurité nationale, sont encore à l'étude au sein des directions concernées par la lutte contre la cybercriminalité. Toutefois, une grande cohérence apparaît déjà entre ces recommandations et les actions mises en oeuvre par le ministère. En effet, à l'échelon ministériel, la cyberdéfense et la protection des systèmes d'information et de communication (SIC) est une priorité qui se traduit, depuis 2011, par la montée en puissance des effectifs et des moyens dédiés à la lutte contre la cybercriminalité au sein des armées, de la direction générale de l'armement (DGA) et des services spécialisés en matière de cyberdéfense. Cette dynamique, qui sera maintenue sur la période 2012-2016, s'inscrit dans un schéma directeur capacitaire pour les années 2013-2020, dont les objectifs seront actualisés lors des prochains travaux sur la loi de programmation militaire. Le dispositif est également caractérisé par une communication accrue auprès du personnel civil et militaire. A cet effet, le ministère de la défense a engagé des actions de sensibilisation aux risques cybernétiques auprès de ses agents, dont la quasi-totalité a signé une attestation de reconnaissance de responsabilité sur l'utilisation des SIC. En outre, une instruction définit depuis 2008 le code d'usage des SIC au sein du ministère. A l'échelon national, la cyberdéfense et la protection des SIC apparaissent également comme une priorité. En effet, le ministère de la défense, acteur majeur du dispositif national, oeuvre à la fois à la protection et la défense de ses propres SIC (notamment ceux déployés en opérations extérieures), et en qualité de principal partenaire de l'agence nationale de sécurité des systèmes d'information (ANSSI). Les moyens déployés par le ministère et l'ANSSI leur permettent d'assurer conjointement une veille permanente relative à la cryptographie, aux technologies de l'information, aux attaques informatiques et aux vulnérabilités matérielles et logicielles des produits et technologies civiles. Le ministère partage également avec l'ANSSI sa connaissance du tissu industriel et des solutions techniques développées par les acteurs nationaux de confiance. Leur coopération sera accrue, d'une part, par la colocalisation, au cours de l'été 2013, du centre d'analyse de lutte informative défensive (CALID) de la défense et du centre

opérationnel de sécurité des systèmes d'information (COSSI) de l'ANSSI ; d'autre part, au travers d'études amont et la mise en place d'une politique industrielle, de formation et de recherche et développement ambitieuse et coordonnée. Enfin, le ministère tisse actuellement des premiers liens techniques entre le CALID et le centre spécialisé en matière de cybercriminalité de la direction générale de la gendarmerie nationale afin de créer un pôle juridictionnel spécialisé à compétence nationale, destiné à réprimer les atteintes graves aux SIC. S'agissant de l'amélioration de la prise en compte de la protection des SIC, une cartographie de l'ensemble des SIC de la défense est en cours d'élaboration par la direction générale des systèmes d'information et de communication (DGSIC) et la direction des réseaux d'infrastructures et des systèmes d'information (DIRISI). De plus, afin de maîtriser les passerelles d'interconnexion de ses réseaux internes avec le réseau Internet, le ministère s'est doté d'instances chargées de rationaliser le nombre de ces passerelles et d'assurer leur sécurité. A ce titre, la réglementation relative à la protection du secret au sein du ministère impose une autorisation du ministre pour l'ouverture de toute nouvelle passerelle vers un réseau exogène. Concernant l'aspect budgétaire de la protection des SIC, le rapport du Sénat recommande de réserver un pourcentage significatif du montant des projets à leur sécurité. Le ministère considère toutefois que le budget alloué à la sécurité doit être établi en fonction du risque et des impacts, dont les évaluations sont réalisées par l'homologation systématique des SIC. Il doit être également souligné que le maintien en condition de sécurité est certes une opération primordiale, mais coûteuse. Par conséquent, les budgets qui y sont consacrés devront être en accord avec cet enjeu ; le coût de la sécurité résidant davantage dans le fonctionnement que dans l'équipement. A l'échelon interministériel, le ministère de la défense participe au renforcement de la direction interministérielle des systèmes d'information et de communication (DISIC). Dans ce cadre, il est responsable de 4 chantiers et participe à 12 autres sous la tutelle de la DISIC. De plus, le ministère a choisi de rejoindre le réseau interministériel de l'État (RIE) afin de concourir à la rationalisation des moyens de l'Etat et de le faire bénéficier de ses capacités de lutte contre la cybercriminalité. Le ministère de la défense s'attache également à promouvoir l'esprit de cyberdéfense dans la sphère civile, notamment auprès des populations, du monde universitaire, du monde industriel et des opérateurs d'importance vitale. S'agissant des populations, après avoir longtemps conduit l'innovation technologique dans de nombreux domaines liés aux télécommunications et aux SIC, la défense nationale doit aujourd'hui se concentrer sur les besoins qui lui sont propres et suivre les développements très rapides menés désormais par le domaine civil. Ceci doit se traduire par des études techniques très réactives, conduites en interne ou externalisées, permettant d'évaluer les technologies émergentes, notamment en termes de sécurité et de robustesse et d'identifier les vulnérabilités potentielles que leur usage peut générer pour la société civile. Par ailleurs, afin de faire rayonner l'esprit de cyberdéfense et de participer à la visibilité des armées au niveau de la population, l'état-major des armées a créé, le 13 juillet 2012, un réseau cyberdéfense de réservistes citoyens, dont la vocation s'inscrit dans une démarche de défense et de sécurité nationale appliquée à la nature transverse du cyberespace. S'agissant du monde universitaire, le ministère contribue à la formation de cadres et d'ingénieurs dans le domaine de la cyberdéfense et de la cybersécurité dans la perspective d'une importante montée en puissance des compétences des armées françaises en la matière. Cela se traduit tant par la formation spécialisée des acteurs que par leur formation opérationnelle. Pour y parvenir, un pôle d'excellence se développe dans la région de Rennes, dans lequel s'inscrit la chaire de cyberdéfense créée en juillet 2012 au sein du centre de recherche des Écoles de Saint-Cyr-Coëtquidan. De plus, depuis deux ans, un module de sensibilisation à la cyberdéfense a été introduit au sein du cursus de formation de l'École de guerre. Enfin, le ministère, qui entretient depuis plusieurs années un lien étroit avec les laboratoires universitaires dans le domaine de la cryptographie, a entrepris un recensement des acteurs compétents dans la lutte contre la cybercriminalité et a initié, avec l'institut de recherche en informatique et en automatique (INRIA), fin 2011, une convention pour le financement de thèses dans le domaine de la cyberdéfense. Ces initiatives se poursuivent actuellement avec d'autres laboratoires ou centres de recherche et doivent se concrétiser prochainement par la mise en place de nouvelles conventions destinées à soutenir la recherche et le développement en ce domaine. S'agissant du monde industriel, le ministère de la défense étudie la possibilité d'imposer à court terme, aux titulaires de ses marchés ainsi qu'à leurs sous-traitants, un certain nombre d'obligations relatives à la cyberdéfense, et notamment celles relatives à une protection accrue des réseaux manipulant des informations classifiées ou liées à la déclaration d'incidents auprès de l'autorité contractante et la direction de la protection et de la sécurité de la défense (DPSD). En outre, le ministère porte une attention particulière aux PME et aux entreprises de taille intermédiaire dans plusieurs domaines stratégiques dont la

cyberdéfense. Cette démarche se décline en plusieurs actions concrètes d'appui aux projets d'innovation, d'animation de la communauté industrielle et académique, et d'accès aux marchés de défense. La politique industrielle conduite par le ministère identifie les domaines technologiques qu'il convient de maîtriser au niveau national, afin de répondre à certaines questions majeures de souveraineté. La cyberdéfense et la protection des systèmes d'information sont directement concernées. Le développement et la pérennisation d'une base industrielle et technique de défense dans ces domaines font l'objet d'un effort permanent. Par ailleurs, le ministère de la défense soutient l'industrie française de la cyberdéfense pour son développement international et encourage une politique industrielle d'exportation volontariste, active et cohérente, mais également responsable. A ce titre, un chargé d'affaire « export, sécurité & cyberdéfense » accompagne les sociétés de sécurité informatique à travers des offres de services étatiques, notamment d'expertise, en cohérence avec les offres industrielles, et développe les coopérations entre gouvernements pour fixer un cadre aux activités industrielles françaises. S'agissant des opérateurs d'importance vitale (OIV), le ministère incite les industriels du secteur « activité de l'industrie de l'armement » à développer la protection et la défense de leurs moyens informatiques ; ces derniers recouvrant les systèmes d'information classiques mais également les systèmes industriels (incluant les systèmes dits « SCADA ») et les systèmes logistiques. Ceci se traduit par des actions d'audit et de conseil, mais également de délivrance d'avis d'aptitude informatique, indispensable pour l'obtention de marchés manipulant des informations classifiées de défense. Une attention particulière est portée à l'architecture des réseaux, de manière à permettre leur défense en maîtrisant leur cartographie, en limitant les passerelles, en gérant le cloisonnement et en positionnant des systèmes de surveillance des flux de manière stratégique et efficace. Cette démarche est cependant rendue difficile, dans la mesure où elle présente un coût certain et s'oppose généralement aux besoins fonctionnels des utilisateurs qui poussent à toujours plus d'interconnexion, de mobilité et de partage de l'information. Une réflexion est également en cours pour intégrer aux OIV certains opérateurs externes critiques pour le soutien de missions relevant des activités militaires de l'État. Enfin, dans le cadre de la lutte contre la cybercriminalité, le ministère de la défense est également engagé dans plusieurs coopérations bilatérales, comme c'est notamment le cas avec nos alliés américains et britanniques avec lesquels nous sommes engagés sur plusieurs théâtres d'opérations, mais aussi avec d'autres puissances avec lesquelles un dialogue est ouvert (rencontres avec la Russie et la Chine en 2012). Bien que le développement de produits de sécurité, notamment cryptographiques, se prête peu à la coopération internationale en raison des fortes implications en termes de souveraineté, la prise en compte des questions de sécurité de l'information et de cyberdéfense s'avère quant à elle indispensable et donnera lieu à un accroissement de ces coopérations, en particulier avec l'Allemagne et le Royaume-Uni, dans le cadre de programmes d'armement conjoints. Par ailleurs, des coopérations au sein de l'Organisation du traité de l'Atlantique Nord (OTAN) et de l'Union européenne (UE) permettent à la France de participer aux travaux d'interopérabilité des mécanismes de sécurité et de réaction commune face aux attaques informatiques. Ces questions sont traitées dans des groupes spécifiques portés par l'OTAN. Le ministère de la défense étudie également la possibilité de contribuer aux travaux du centre d'excellence OTAN pour la cyberdéfense en coopérations de Tallin, en Estonie. Enfin, au sein de l'Organisation des Nations unies (ONU), le ministère de la défense et le ministère des affaires étrangères participent conjointement aux travaux du groupe d'experts gouvernementaux qui se réunissent dans le cadre de la première commission de l'ONU, dont l'un des axes de travail consiste à développer un éventail de normes de comportement non contraignantes, visant à renforcer la confiance entre les États au sein du cyberespace. Ainsi, le ministère de la défense continue de soutenir son effort en matière de lutte contre la cybercriminalité, étant précisé que la protection de ses systèmes d'information et de communication est une nécessité pour la réalisation des missions qui lui sont confiées. Par ailleurs, le ministère joue un rôle structurant dans le dispositif national de cyberdéfense. Il possède des capacités lui permettant de promouvoir l'esprit de cyberdéfense dans la sphère civile et représente aujourd'hui un acteur essentiel du développement du réseau de dialogue national et des coopérations internationales. Toutefois, la mise en oeuvre de la plupart des recommandations du récent rapport du Sénat sur la cyberdéfense est conditionnée par la disponibilité de moyens financiers et surtout humains. Le futur livre blanc sur la défense et la sécurité nationale, ainsi que la loi de programmation militaire qui en découlera, encadreront plus précisément les affectations de ressources nécessaires à la cyberdéfense et la protection des SIC.