ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

Mercredi
12 juin 2013
Séance de 17 heures 30

Compte rendu n° 79

SESSION ORDINAIRE DE **2012-2013**

Présidence
de Mme Patricia Adam,
présidente

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-sept heures trente.

Mme la présidente Patricia Adam. Je suis heureuse d'accueillir le contre-amiral Arnaud Coustillière, officier général en charge de la cyberdéfense à l'état-major des armées.

Nous débutons ainsi le cycle de nos travaux dans le cadre de la loi de programmation militaire. En effet, dans l'attente du texte de ce projet, annoncé pour la fin du mois de juillet, il est possible de commencer à travailler sur certains sujets qui feront à l'évidence partie des débats de cet automne, et la cyberdéfense est assurément l'un d'entre eux. Aussi, sans plus attendre, je vous laisse la parole, amiral.

Contre-Amiral Arnaud Coustillière. Le phénomène le plus frappant est la grande rapidité d'évolution de la menace. L'actualité est marquée par les accusations mutuelles entre les États-Unis et la Chine. Ces deux États dialoguent, sans d'ailleurs laisser d'espace aux autres puissances, fût-ce la Russie. Cela donne le sentiment d'un monde à nouveau bipolaire.

On peut s'interroger sur la rapidité avec laquelle cet enjeu de la cyberdéfense est venu sur le devant de la scène, ainsi que sur les raisons motivant les crispations actuelles. Il faut noter qu'au-delà des divergences culturelles, les enjeux sont surtout économiques. De ce point de vue, l'Europe pourrait se trouver laminée, et avec elle sa puissance industrielle dans ce domaine ainsi que les données personnelles de ses citoyens.

Je travaille sur ces questions depuis 2008. J'ai vu depuis cette époque combien, à chaque étape, les rapports parlementaires ont contribué à la prise de conscience du besoin : le rapport de Pierre Lasbordes en 2006, qui a débouché sur la création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), le rapport de Roger Romani en octobre 2008, préfigurant le Livre blanc de 2008 et la loi de programmation militaire (LPM) qui a suivi, qui ont vu l'émergence d'une communauté française du cyber. Celle-ci réunit toutes sortes d'acteurs au sein du ministère de la Défense ainsi que le secrétariat général de la défense et de la sécurité nationale (SGDSN) et l'ANSSI. Leurs travaux en commun ont permis de construire un modèle correspondant à notre culture. Nous pouvons aborder aujourd'hui une nouvelle étape. Si le Livre blanc de 2008 était un initiateur, celui de cette année pose les pierres fondatrices pour la mise en place de nouvelles capacités et l'adoption d'une nouvelle approche de cet espace. Si nous avons aujourd'hui un dispositif équilibré, il reste un certain nombre de sujets encore trop peu abordés : la politique industrielle de la France et de l'Europe, la politique d'éducation et de formation au cyber, ainsi que les enjeux juridiques et législatifs.

Le cyber espace est désormais reconnu comme un milieu à part entière. Il peut donc être comparé aux autres dans leur complexité ; par exemple le milieu maritime qui connaît un droit spécifique, un droit du commerce maritime, le phénomène de la piraterie, des problématiques de circulation des flux, etc.

Nous ne pouvons nous satisfaire de la façon dont le problème a été abordé dans sa dimension verticale : développement de la société numérique, des problématiques de cybercriminalité, tandis que le dispositif juridique de protection des données personnelles s'améliore. En revanche, notre pays manque toujours d'un étage global à son dispositif, assurant sa cohérence. Le traitement de cette question devrait conférer un rôle central aux parlementaires.

Depuis ma prise de fonctions en 2011, j'occupe une double fonction : officier général en charge de la montée en puissance des capacités de cyberdéfense des armées françaises, d'une part, et chef cyber du centre de planification et de conduite des opérations (CPCO), d'autre part. À ce titre, je suis en charge d'assurer la défense de l'ensemble des systèmes d'information du ministère de la Défense et la synchronisation des actions informatiques d'accompagnement des actions militaires. Bien les coordonner et garantir un résultat précis aux autorités est particulièrement difficile, d'une complexité sans commune mesure avec l'action ponctuelle des *hackers*.

Au sein du ministère, je travaille en étroite collaboration avec l'ingénieur en chef Guillaume Poupard, responsable du pôle de sécurité des systèmes d'information à la DGA, qui assure, à ce titre, l'interface avec les équipes techniques de Bruz.

Nous entretenons également une relation particulièrement étroite avec l'ANSSI, dans le cadre d'un protocole qui nous lie à l'agence. Elle nous alimente en renseignement d'alerte et nous l'appuyons notamment dans son travail de sensibilisation.

Au-delà, à l'échelle du ministère, nous avions constaté au cours d'incidents en 2009 que nous ne disposions pas d'une structure capable de gérer la défense réactive face à des « infections informatiques » de grande ampleur, chaque grande direction agissant de façon pas assez coordonnée. Cela explique l'attribution au CEMA de cette responsabilité de défense réactive, qui la délègue ensuite à l'officier général en charge du cyberespace. De son côté, l'ANSSI a connu une véritable montée en puissance dans les domaines de l'intervention et de la protection des réseaux, notamment depuis les attaques contre l'entreprise Areva et contre le ministère des finances. Le CPCO a vu quant à lui croître la part de son activité consacrée à la cyberdéfense et son rôle de tête de chaine opérationnelle.

Le plan de montée en puissance des capacités cyber se poursuit. Le ministère compte actuellement 1 600 personnels investis dans cette question, dont 1 200 relevant de l'EMA, avec 300 personnels en charge des équipements de chiffrement et 900 du seul périmètre cyber, pour la chaine de protection/prévention et à présent celle plus récente de défense des systèmes. Sur ces 900 personnels, environ 60 s'occupent des métiers très pointus de l'expertise et de l'audit, 70 de la lutte informatique défensive et tous les autres s'occupent de prévention, de l'exploitation, ou de l'architecture des systèmes.

La LPM à venir devrait confirmer le plan d'augmentation des effectifs à hauteur de 350 personnels, notamment pour assurer des missions de prévention et de défense. Actuellement, les exigences de la protection des réseaux sont bien perçues et l'on sait comment renforcer très rapidement leur sécurité. Ce que l'on connaît moins bien réside davantage dans les systèmes d'armes et les automatismes embarqués dans les systèmes automatisés. Une FREMM par exemple rassemble 2 400 systèmes d'information ! Comment « encapsuler » ces systèmes ? Tel est bien l'objet des renforcements prévus pour les années 2014-2015.

Mme la présidente Patricia Adam. J'aimerais que vous évoquiez devant nous l'aspect européen de la cyberdéfense. Ce sujet revient souvent dans les discussions avec nos partenaires et j'ai l'impression qu'il sera plus facile de le faire avancer que celui de l'Europe de la défense.

Contre-amiral Arnaud Coustillière. Avant d'évoquer l'aspect européen, je voudrais parler de l'approche de l'OTAN en la matière. C'est un sujet dont elle s'est saisie depuis novembre 2010 et elle s'est dotée très rapidement d'un concept et d'une politique. Mais, depuis cette date, plutôt que de chercher à l'approfondir avec nos partenaires de l'Alliance pour mettre en place une capacité de gestion de crise, l'OTAN tente plutôt d'ouvrir des dialogues avecde nouveaux, comme la Russie par exemple ; le processus est aujourd'hui moins dynamique.

Une des questions en suspens est de savoir quand l'OTAN aura la capacité de protéger ses propres réseaux. Son secrétaire général a déclaré très récemment que l'Alliance s'était dotée d'une équipe d'intervention rapide, mais celle-ci n'est dotée pour l'instant que de 6 personnes destinées aux seuls réseaux de l'OTAN ! Les effets d'annonce masquent en réalité des capacités réduites.

Par ailleurs, une divergence de fond entre les différents partenaires n'est aujourd'hui pas résolue. Certains pays, dont les principales nations européennes, souhaitent que l'OTAN se concentre sur ses propres capacités militaires. D'autres, plus petits, souhaiteraient que l'OTAN prenne en charge la protection de leurs réseaux d'importance vitale. Cette divergence sur le rôle de l'OTAN dans ce domaine est un frein à l'approfondissement de ses capacités, malgré la volonté affichée par le secrétaire général.

L'Union européenne doit faire de la cyberdéfense une de ses priorités et s'occuper notamment de la protection de ses infrastructures vitales. Cette question concerne aussi sa politique industrielle, car il faudrait qu'elle développe ses propres capacités d'hébergement des données pour ne pas être totalement dépendante des firmes américaines. L'Union a adopté récemment une directive stratégique, ce qui constitue une avancée majeure car cela signifie qu'elle s'est réellement saisie de ce sujet. Trois comités ministériels importants vont se tenir à partir de septembre et il faudra en profiter pour le faire avancer : l'un sera consacré à la politique de sécurité et de défense commune, un autre à l'industrie et le troisième à l'économie numérique.

M. Joaquim Pueyo. Le secrétaire général de l'OTAN a déclaré que la capacité d'intervention de l'Alliance serait pleinement opérationnelle l'automne prochain. Qu'en est-il réellement ? L'Union européenne semble se doter d'une stratégie complète : quels leviers peuvent la faire avancer ? Vous y avez déjà répondu pour partie, mais le sujet peut être approfondi. Enfin, le Livre blanc souhaite confier des tâches nouvelles à la réserve citoyenne en matière de cyberdéfense : ne vaudrait-il pas mieux renforcer la formation du personnel de carrière ?

Contre-amiral Arnaud Coustillière. Le secrétaire général de l'OTAN faisait référence au centre de supervision des réseaux de l'OTAN, qui sera effectivement opérationnel cet automne au plus tôt. Ce centre supervisera quelques dizaines de milliers postes de travail, soit un dixième en gros de ce que supervise aujourd'hui le ministère de la Défense. Les annonces sont importantes mais les résultats concrets le sont moins… L'OTAN reste une bonne enceinte de discussion avec nos partenaires, mais sa capacité d'action propre demeure aujourd'hui très faible.

De quels leviers dispose aujourd'hui l'Union européenne ? Les 27 sont d'accord sur les menaces et l'importance de la cybersécurité. Mais la volonté de développer et protéger

l'industrie face à l'espionnage, et en particulier les PME n'est pas unanimement partagé pour l'instant et, de ce point de vue, la présidence irlandaise de l'Union n'a pas permis de progresser. Avec le Royaume-Uni, l'Allemagne et l'Estonie, et quelques autres nations particulièrement investies, nous essayons sous l'égide du ministère des Affaires étrangères de faire avancer ce dossier et les trois réunions de l'automne prochain seront très importantes à cet égard. Il faudrait aussi que les instances de normalisation de l'OTAN et de l'Union européenne se rapprochent. Le centre de Tallin, par exemple, subit une forte influence des conceptions juridiques américaines sur la défense préemptive ; y apporter un peu de droit européen serait des plus souhaitables.

Pour ce qui concerne l'utilisation des réserves citoyennes, j'assume une grande part de la paternité de cette idée. Celle-ci est issue du retour d'expérience que nous avons fait de l'intervention de l'ANSSI à Bercy, après les cyberattaques que ce ministère avait subies. L'ANSSI y avait fait intervenir, dans un premier temps un groupe d'intervention rapide composé de quelques spécialistes et ingénieurs de très haut niveau pour l'audit et le diagnostic. Puis, dans un deuxième temps, elle a envoyé une trentaine d'ingénieurs de haut niveau pour mettre en place les plans de reprise et de reconquête du réseau. Cette dernière a mobilisé environ 300 administrateurs de réseau. Aujourd'hui au sein des armées, le vivier d'ingénieurs de très haut niveau capables d'intervenir en premier est de l'ordre de 200 personnes, sur les 6 000 personnels des SIC que comprend la DIRISI. C'est une compétence rare, que seul l'État et quelques grandes entreprises sont capables de posséder, et surtout de mobiliser rapidement en les faisant rapidement basculer de priorité d'emploi. Au deuxième niveau de l'intervention, nous avons besoin d'un personnel très nombreux pour redéployer un réseau. Le vivier est là de l'ordre de 700 à 800 personnes.

La question que l'on s'est posée à la suite de cet événement est donc : comment s'organiser pour la phase de reconquête après une éventuelle attaque d'ampleur à l'échelle d'une ville par exemple ? C'est ici que les réserves peuvent avoir un rôle intéressant. La réserve citoyenne offre un cadre juridique existant, qui garantit une sécurité de recrutement et administrativement aisé à mettre en place, mais sa mission se limite à de la réflexion et à de la promotion autour de la cyberdéfense, et son statut interdit son emploi dans des fonctions opérationnelles. Aujourd'hui, nous avons 75 réservistes citoyens, dont les trois quarts, ingénieurs, informaticiens, sont des praticiens de la cyberdéfense. Les autres sont des journalistes, des élus ou des juristes. Nous avons monté sept groupes de travail – l'un tourné vers des hautes personnalités, un autre qui travaille sur la sensibilisation des PME-PMI à ces questions, par exemple – qui nous permettent de disposer d'un véritable réseau en développement en région, chargé de la sensibilisation des acteurs.

La réserve opérationnelle est actuellement moins adaptée à un besoin en cas de crise car on n'y trouve qu'assez peu de personnes compétentes et surtout disponibles sous faible préavis dans les domaines qui nous intéressent. Pour répondre à une crise majeure où des dizaines de milliers de postes de travail doivent être revus, il faut un plan de secours en trois niveaux : le premier, qui fait appel à des experts très qualifiés, relève à mon sens des compétences de l'État ; le deuxième fait appel à du personnel des sociétés privées ou à des cadres issus de la réserve ; le troisième enfin, que nous essayons de construire et qui nécessite de gros contingents, s'adresse plus à des étudiants en formation de niveau licence-master ou à du personnel de niveau « administrateur réseau » qu'il faut encadrer. C'est précisément ce troisième niveau que le Livre blanc veut promouvoir et que nous allons développer à partir

des travaux menés par la réserve citoyenne, et avec les différents partenaires interministériels et des différents ministères concernés.

M. Éduardo Rihan Cypel. Dans le prolongement du Livre blanc de 2008 qui abordait pour la première fois la notion de cyberdéfense, le nouveau Livre blanc introduit une volonté normative et régulatrice à l'endroit des quelque deux cents opérateurs d'importance vitale (OIV) publics et privés. Quel est votre avis sur la manière de procéder ?

Le discours prononcé à Rennes par le ministre de la Défense marque un tournant majeur, amorcé dans le Livre blanc, en affirmant que la France doit non seulement élaborer une doctrine défensive en matière de cyberdéfense mais bien se doter de capacités offensives. Sommes-nous prêts et existe-t-il une différence technique entre capacités défensives et offensives ?

Contre-amiral Arnaud Coustillière. Il s'agit effectivement d'un discours fondateur. La prochaine LPM offrira le support juridique permettant de doter l'ANSSI du pouvoir de donner des directives aux OIV. Aujourd'hui les OIV ne sont pas tenus de déclarer les attaques qu'ils subissent. Or les victimes ont tendance à assimiler l'attaque à une incompétence de leur part et à adopter une posture de déni, de dissimulation, voire de honte. Les entreprises déclarant ne jamais avoir été attaquées sont soit naïves, soit déjà pillées, donc moribondes. S'il est impossible d'empêcher toutes les tentatives d'attaque, on peut toutefois les détecter et les contrer. Il faut pour cela être en mesure de reconnaître l'attaque dans un cercle de confiance et chercher l'aide d'organismes compétents. La LPM devrait consacrer le rôle de l'ANSSI sur ce plan et lui donner les pouvoirs nécessaires, sous l'autorité du Premier ministre, tout en laissant la possibilité à chaque ministère de travailler à sa cybersécurité en concertation avec l'agence. Dans la LPM, un article confortant la notion de motif légitime du code pénal devrait concerner le ministère de la Défense, et peut-être certains autres ministères régaliens, les autorisant, en cas d'attaque avérée, non seulement à enquêter au sein de leur propre système, comme c'est le cas aujourd'hui, mais à interagir avec l'attaquant, ce que le code pénal ne permet actuellement pas sauf via cette clause de motif légitime soumise aux aléas jurisprudentiels.

Le Livre blanc ébauche une doctrine de dissuasion classique face aux attaques informatiques : renforcement de la posture de défense par l'action de l'ANSSI et la coopération interministérielle sous l'autorité du Premier ministre et, en cas d'attaque majeure contre les intérêts stratégiques de l'État, réponse par tous les moyens de l'État, policiers, juridiques, diplomatiques ou coercitifs relevant du ministère de la Défense. Il n'y a pas de lien entre la nature d'une attaque et la nature de la réponse, il ne sera donc pas répondu systématiquement à une attaque informatique par une attaque de même type. Le cyberespace est un espace « gris » en proie à une prolifération galopante dans lequel les attaquants ne sont pas facilement identifiables et les acteurs aussi nombreux que variés. Les principes de la dissuasion nucléaire ne peuvent de ce fait s'appliquer au cyberespace.

Les capacités offensives évoquées dans le Livre blanc existent. Le volume des forces, leur organisation et les ambitions fixées sont des informations qui relèvent du secret défense mais je suis en mesure de vous dire que nous ne sommes pas dépourvus.

M. Christophe Guilloteau. Le Livre blanc évoque la sensibilisation des collectivités territoriales, auxquelles, comme j'ai pu le constater, le domaine de la cybersécurité est

souvent étranger. Comment sera-t-elle mise en œuvre ? Par ailleurs, où se situe la frontière entre vos compétences et celles de l'ANSSI ?

Contre-amiral Arnaud Coustillière. Les périmètres de responsabilité sont sans ambiguïté. L'ANSSI est l'autorité gouvernementale sur l'ensemble des ministères et des OIV. Le ministère de la Défense, qui doit avoir un niveau de résilience supérieur à celui des autres ministères, occupe une place particulière et doit assurer sa cybersécurité de façon autonome. Il apporte à l'ANSSI sa contribution *via* le renseignement spécialisé transmis par ses services de renseignement, la cryptologie de niveau souveraineté, le développement de produits de sécurité souverains, l'expertise de la DGA, le suivi des OIV qui en dépendent et l'assistance de la direction de la protection et de la sécurité de la défense (DPSD).

Les relations avec l'ANSSI sont très étroites, à telle enseigne que le centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI va bientôt emménager dans des locaux situés en bord de Seine et accueillir le centre opérationnel du ministère de la Défense. L'ANSSI développe également des produits souverains, des sondes notamment, utilisées pour surveiller les ministères dont celui de la défense. Dans le cadre de relations institutionnelles internationales l'ANSSI représente l'autorité gouvernementale à laquelle s'associe le ministère de la Défense. Des experts de l'ANSSI peuvent également accompagner les représentants du ministère de la Défense en tant que de besoin, et vice versa.

M. Sylvain Berrios. Vous avez abordé les capacités offensives et défensives, mais il est également un autre volet : la capacité préventive. L'actualité récente montre que le gouvernement américain s'est octroyé un pouvoir d'espionnage très large des données personnelles par l'intermédiaire de grandes firmes américaines opérant dans le secteur de l'Internet. Cela pose naturellement la question de la protection de nos données personnelles et de l'architecture de nos systèmes. En 2009, une de ces grandes compagnies américaines a bénéficié d'un accord-cadre avec le ministère de la Défense, à l'issue duquel devait normalement être mise en place en 2011-2012 une solution basée sur l'utilisation de logiciels libres, permettant ainsi d'avoir un meilleur accès aux codes sources et conférer ainsi d'une capacité préventive accrue. Pouvez-vous nous donner votre point de vue sur cette question ?

Contre-Amiral Arnaud Coustillière. De manière générale, les pays anglo-saxons ont choisi de confier l'ensemble de leur cyberdéfense aux services de renseignement. Cela ne correspond pas à notre culture et, en France, un partage des tâches est opéré entre les services de renseignement, d'une part, et l'ANSSI et mes services, d'autre part. Pour reprendre la comparaison avec les milieux, ce qui nous intéresse c'est en quelque sorte le contenant, les métadonnées, tandis qu'il appartient aux services de renseignement de caractériser les intentions et objectifs, le contenu. Ce partage me paraît sain.

S'agissant de l'utilisation des données personnelles confiées par les utilisateurs à de grandes sociétés opérant dans le domaine de l'Internet, il convient de relever le paradoxe entre cette remise volontaire par tout un chacun et le fait qu'en France l'État ne peut accéder à ces données que de manière extrêmement encadrée, sous le contrôle étroit de la CNIL. En ce qui concerne la prévention, les grands éditeurs de logiciels, dont les produits ont tendance à devenir des normes, ne sont pas forcément moins bons en matière de sécurité de leurs produits que les développeurs de logiciels libres. Ils ont en effet tout intérêt à faire évoluer leur produit commercial et à en assurer la fiabilité dans la durée. Inversement, le logiciel libre est

développé par une communauté, parfois à géométrie variable. En tout état de cause, le débat entre logiciel commercial et logiciel libre tourne parfois à la « guerre de religion ».

Le ministère de la Défense a fait le choix d'un accord-cadre avec Microsoft, ce qui, de mon point de vue, ne présente pas un risque de sécurité supérieur par rapport à l'utilisation de logiciels libres. Dans ce dernier cas, il aurait fallu développer une capacité forte de suivi et de contrôle pour se garantir effectivement contre les risques éventuels. En la matière, il convient d'adopter une approche mesurée et pragmatique, tenant compte à la fois du coût, des risques et de contraintes opérationnelles, dont notamment le lien avec l'OTAN. On peut en outre constater que ce débat sur les logiciels libres a permis d'engager une baisse tendancielle des prix pratiqués par les grands éditeurs de logiciels et, parallèlement, à une décroissance du recours aux logiciels libres.

Ces éléments ne doivent pas être interprétés comme l'expression d'une forme de naïveté. Les risques de sécurité sont de plusieurs ordres. Évidents en cas de réseau connecté directement sur Internet, ils sont davantage mesurés lorsque des passerelles filtrées sont mises en œuvre. Les attaques d'espionnage utilisent moins les failles éventuelles de produits Microsoft que celles de documents en format Pdf ou de logiciels de développements de sites. Enfin, s'agissant des réseaux classifiés, sans aucun contact physique avec des réseaux extérieurs, le risque d'attaque extérieure est en théorie plus faible, mais leur sécurité repose plus largement sur le comportement des utilisateurs, tout particulièrement en ce qui concerne l'usage des clés USB.

M. Jean-Yves Le Déaut. Après la récente affaire Snowden sur le cyber espionnage, ne trouvez-vous pas que nous restons un peu naïfs vis-à-vis des États-Unis et donc de Microsoft ? Quels sont les risques supplémentaires induits par le développement de la technique de stockage en nuage ? On peut constater effectivement que la coopération entre entités administratives, sous l'autorité de l'ANSSI, se développe de manière satisfaisante. Toutefois, comme vous l'avez relevé, certaines attaques continuent à ne pas être déclarées. Quelle est votre évaluation de l'évolution du nombre d'attaques et la meilleure coordination du dispositif français permet-elle d'ores et déjà de constater des résultats en la matière ? Enfin, je m'inquiète de la part consacrée à la R&D pour faire face à cette menace et aux liens insuffisants entre les acteurs, notamment avec les universités. Formons-nous suffisamment d'ingénieurs dans ce domaine ? Ne pensez-vous pas qu'il faille développer également la sensibilisation des utilisateurs en renforçant la formation à la cyber sécurité dans les écoles d'administration et les écoles militaires ?

M. Gwendal Rouillard. Je précise qu'un projet sur la cyberdéfense est en cours de création et associe le ministère de la Défense, le centre DGA de Bruz et l'école d'ingénieurs de l'université Bretagne-Sud. Plus généralement, quelle est la part de l'effort de recherche en la matière qui sera attribuée à des PME-PMI ? Quelle est l'ampleur de l'effort à consentir pour une sensibilisation la plus large possible des utilisateurs aux questions de sécurité des systèmes d'information ?

Contre-Amiral Arnaud Coustillière. Sur ces points, il faut bien convenir que nous avons encore du retard sur nos partenaires anglo-saxons. Cependant, je me dois de relever que nous avons obtenu les moyens budgétaires supplémentaires que nous demandions. Les insuffisances sont donc davantage liées à un problème général de disponibilité de la ressource humaine au bon niveau de compétence. On observe qu'il est difficile d'attirer des étudiants

vers les formations sur ce sujet et que de surcroît, une bonne part des élèves qui y sont formés sont de nationalité étrangère, ce qui limite les possibilités ultérieures de recrutement par des intervenants dans les domaines régaliens, tandis qu'environ 15 % des diplômés d'écoles spécialisées sont très rapidement recrutés par des sociétés américaines. La ressource reste en conséquence nettement inférieure aux besoins et un effort d'ampleur doit être organisé.

En ce qui concerne les crédits de R&D, une progression très significative a été annoncée par le ministre, les crédits devant tripler, pour atteindre un montant total de 30 millions d'euros. On observera qu'en 2009, ces crédits étaient tombés à 3 millions d'euros. Plus largement, l'une des missions principales que s'est fixée la DGA réside dans la consolidation de l'« écosystème » de la cyberdéfense ; elle peut s'appuyer sur une véritable prise de conscience de l'importance du sujet.

Concernant l'école de Rennes, nous réfléchissons au sein du ministère de la Défense à la viabilité économique du projet et justement à sa rapide consolidation. Nous voulons que la formation soit complète tant sur les aspects juridiques que la gestion de crise, par exemple. Nous réfléchissons aussi à la création d'une pépinière d'entreprises, la création d'un colloque annuel, sur le modèle des universités d'été de la défense, qui verrait intervenir doctorants et intervenants de haut niveau. Il y a donc aujourd'hui un foisonnement de réflexion autour de ce projet, qui associe aussi la DGA, différents partenaires et les réseaux de réservistes citoyens que j'ai évoqués tout à l'heure. Cette école constituerait un outil supplémentaire pour sensibiliser aux questions de cybersécurité et le creuset de nos capacités.

Avec l'OTAN, nous coopérons énormément, nous avons déjà évoqué ce sujet. Avec les États-Unis, notre relation est compliquée. Nous partageons pour l'essentiel les mêmes valeurs et intervenons ensemble sur de nombreux théâtres d'opération. Mais, dans le même temps, nous sommes en compétition sur de nombreux marchés de haute technologie. L'espionnage industriel a toujours existé. Notre relation est donc plus ambiguë.

M. Jean-Yves Le Déaut. Je ne partage votre optimisme sur la question des codes-sources. Nous n'avons jamais rien obtenu de Microsoft. Je pense que l'utilisation de logiciels libres offre plus de garanties.

Contre-Amiral Arnaud Coustillière. Je ne sais pas si le débat se situe toujours là aujourd'hui en termes de sécurité. Ce qui pousse la technologie vers le haut désormais, ce sont les *smartphones*, les informations que l'on trouve sur les *clouds*. Ces systèmes sont extrêmement complexes et les codes sources n'en constituent qu'un élément.

Commandant Hervé Mermod, chef du centre d'analyse en lutte informatique défensive du ministère de la Défense (CALID). Pour essayer de compléter les propos de l'amiral, je dirais que les matériels sont aujourd'hui également concernés par les attaques informatiques et l'enjeu se situe davantage sur ce point que dans la maîtrise des codes sources. Les risques se situent dans les nombreux périphériques de systèmes d'information globaux dont le logiciel ne constitue qu'une brique. D'où la politique menée par la DGA et visant à développer des équipements de confiance nationaux en périphérie permettant de maîtriser les risques relevant des systèmes et matériels. On a en effet pu constater des attaques par des portes dérobées installées sur des cartes réseaux ou des clés 3G de fabrication étrangère.

M. Paul Molac. Sans être un spécialiste du sujet, je note que l'école spéciale militaire de Saint-Cyr Coëtquidan développe un projet de formation de ses élèves sur le sujet de la cyberdéfense.

La séance est levée à dix-neuf heures.

*

* *

Membres présents ou excusés

Présents. - Mme Patricia Adam, M. Sylvain Berrios, M. Daniel Boisserie, M. Jean-Jacques Bridey, Mme Édith Gueugneau, M. Christophe Guilloteau, M. Jean-Yves Le Déaut, M. Paul Molac, M. Joaquim Pueyo, M. Eduardo Rihan Cypel, M. Gwendal Rouillard, M. Michel Voisin

Excusés. - M. Ibrahim Aboubacar, M. François André, M. Olivier Audibert Troin, M. Claude Bartolone, M. Philippe Briand, M. Jean-Jacques Candelier, M. Alain Chrétien, M. Jean-David Ciot, M. Yves Foulon, Mme Geneviève Gosselin-Fleury, M. Serge Grouard, M. Éric Jalton, M. Charles de La Verpillière, M. Bruno Le Roux, M. Maurice Leroy, Mme Sylvie Pichot, Mme Marie Récalde, M. Jean-Michel Villaumé