ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

Mercredi
10 juillet 2013
Séance de 16 heures 30

Compte rendu n° 85

SESSION EXTRAORDINAIRE DE 2012-2013

Présidence
de Mme Patricia Adam,
présidente

ASSEMBLÉE NATIONALE

La séance est ouverte à seize heures trente.

Mme la présidente Patricia Adam. La cyberdéfense sera l'un des grands enjeux des années à venir : nous voulions donc vous entendre dans le cadre de la préparation de la prochaine loi de programmation militaire.

Ingénieur en chef de l'armement Guillaume Poupard, responsable du pôle de sécurité des systèmes d'information à la Direction générale de l'armement. Merci de me donner l'occasion d'expliquer ce que fait la direction générale de l'armement (DGA) en matière de cyberdéfense. Ce n'est pas un sujet neuf, mais il évolue très rapidement. Nous nous efforçons d'avoir tous les moyens techniques pour suivre ces menaces et y répondre.

Je commencerai par dire quelques mots de notre organisation. L'Agence nationale de la sécurité des systèmes d'information (ANSSI), dirigée par M. Patrick Pailloux et placée sous l'autorité du Premier ministre, s'occupe de toutes les questions interministérielles, et épaule de plus en plus ceux que nous appelons des « opérateurs d'importance vitale », publics ou privés, dont la sécurité est essentielle pour la Nation. Elle se charge à la fois des aspects techniques et opérationnels.

Le ministère de la Défense est un peu à part, car le nombre de systèmes qu'il doit protéger est considérable – qu'il s'agisse de systèmes classiques comme des réseaux informatiques, installés sur notre territoire ou déployés en opérations extérieures, ou de systèmes d'armes, potentiellement vulnérables. Au sein du ministère, une mission opérationnelle est chargée de répondre aux attaques ; elle est dirigée par le contre-amiral Arnaud Coustillière et notamment armée par le CALID, centre d'analyse en lutte informatique défensive. Le pendant technique de cette mission opérationnelle est confié à la DGA, au pôle « sécurité des systèmes d'information » dont je suis le responsable et qui traite plus largement de tous les aspects de la cyberdéfense et de la cybersécurité en général. Ce pôle technique est en grande partie installé à Bruz, près de Rennes, au centre DGA Maîtrise de l'information, qui concentre de vastes capacités d'expertise dans divers domaines liés aux technologies de l'information. Cette séparation entre technique et opérationnel fonctionne très bien dans la pratique ; nous entretenons des liens forts, quotidiens, qui vont jusqu'à des échanges de personnels.

Nos liens avec l'ANSSI sont forts et anciens : il n'y a pas là de séparation entre civils et militaires. Nous travaillons ensemble pour concevoir et réaliser des produits de sécurité, notamment en réponse à des besoins de souveraineté, en matière de cryptographie par exemple. Le développement est réalisé par la DGA, avec des industriels et l'approbation, en vue de classification défense, est faite par l'ANSSI : cette organisation est bien rodée.

Nous travaillons évidemment avec d'autres ministères ainsi qu'avec des laboratoires de recherche. La coordination de tous ces acteurs nous permet, nous l'espérons, d'apporter une réponse efficace aux enjeux de cyberdéfense.

Une partie de nos activités relève de la sécurité des systèmes d'information classiques : il s'agit de spécifier des besoins en termes de protection de l'information au sein des réseaux pour les Forces, mais également pour répondre aux besoins interministériels. Nous développons ensuite les produits que l'on ne trouve pas sur étagères, en raison de leur niveau d'assurance élevé qui leur permet de protéger de l'information classifiée de défense.

Pour reprendre l'exemple cité précédemment, nous concevons nos propres mécanismes de cryptographie : c'est un domaine très sensible et la France fait partie des quelques pays au monde à même de mener à bien ces tâches. Il en va de même pour les composants électroniques de sécurité, que nous savons produire nous-mêmes, ce qui est indispensable pour construire des systèmes vraiment fiables. En relation étroite avec certains industriels de confiance, nous réalisons donc ces équipements qui permettent de sécuriser les systèmes d'information comme les systèmes d'armes.

Commentaire [v1]: Pas de raisons d'en tirer un quelconque bonheur… Parler plutôt d'un maintien de souveraineté, ou d'une garantie de sécurité

Par ailleurs, nous nous efforçons d'améliorer notre connaissance de la menace, afin de l'anticiper au mieux. En matière de cyberdéfense, il faut être extrêmement modeste : il est difficile de se protéger des menaces que l'on ne connaît pas. Nous sommes plus sûrs de nous dans certains domaines comme la cryptographie où nous sommes capables aujourd'hui de construire des algorithmes que nous savons être très robustes grâce à des systèmes de preuves mathématiques. Dans le domaine des attaques informatiques en général, il n'y a pas « d'échelle de mesure » : nous essayons de nous défendre des menaces que nous connaissons, et c'est déjà beaucoup. C'est pourquoi nous nous efforçons de bien connaître la menace potentielle et d'anticiper les attaques et restons donc plutôt optimistes.

Enfin, nous avons absolument besoin de disposer d'industriels de confiance capables de réaliser nos systèmes : c'est un aspect que l'on ne peut pas laisser au hasard. Nous finançons donc des travaux de recherche et développement (R&D). Nous travaillons avec des laboratoires académiques – la recherche est riche en France dans le domaine de la sécurité – en finançant des thèses et des travaux de recherche au moyen de conventions. Nous soutenons également des PME : les projets RAPID (régime d'appui à l'innovation duale) les aident à développer des technologies innovantes, qui deviendront des solutions intéressantes pour demain. Ces projets RAPID représentent environ trois millions d'euros par an dans le domaine de la cyberdéfense. Enfin, de longue date, la DGA finance des « études amont » : ce sont des contrats de R&D que nous passons avec des industriels et des laboratoires académiques et qui nous permettent de préparer le futur, d'identifier des risques ou de lever des verrous technologiques, afin de dégager de nouvelles voies de développement et de monter en gamme. Ils sont, en matière de cybersécurité, en croissance très forte : il y a deux ans, nous étions à 10 millions d'euros par an ; notre budget sera pour cette année d'environ 22 à 23 millions d'euros ; à court terme, nous pensons atteindre 30 millions d'euros par an. M. le ministre a confirmé l'importance de ces études lors de sa récente visite à Rennes.

Notre premier sujet d'intérêt est la sécurité des systèmes d'information et de communication. Notre niveau de maîtrise nous rend relativement confiants. Nous travaillons beaucoup, en particulier, sur l'architecture des réseaux.

Nous travaillons aussi sur la sécurité des systèmes d'armes, qui évolue très rapidement : ces systèmes sont de plus en plus complexes, de plus en plus interconnectés et intègrent de plus en plus souvent des briques technologiques acquises sur étagères car on ne peut plus tout redévelopper, et ce ne serait de toute façon pas efficace. Ces systèmes sont donc dans le principe de plus en plus vulnérables à des attaques qui viendraient de l'extérieur et qui toucheraient des composants utilisés dans le domaine civil comme dans le domaine militaire. Sur les anciens systèmes d'armes, nous sommes assez sereins, la notion de cyberattaque ne s'appliquant que difficilement, et nous travaillons donc à parer les attaques potentielles sur les nouveaux matériels, même si elles devaient venir d'adversaires de très haut niveau.

Le troisième domaine sur lequel nous travaillons est celui des systèmes industriels, parfois appelés SCADA (*supervisory control and data acquisition*, c'est-à-dire télésurveillance et acquisition de données). L'affaire Stuxnet, du nom de l'attaque présumée contre les centrales d'enrichissement iraniennes, a montré la réalité de ces menaces. Ces systèmes industriels sont en effet présents partout, chez les opérateurs privés, mais aussi dans tous les équipements civils ou militaires : un navire militaire compte aujourd'hui de très nombreux automates directement issus du domaine civil, qu'il faut protéger. Nous travaillons également sur les infrastructures accueillant ces plateformes militaires.

Les questions de cybercriminalité – toutes les attaques assez simples techniquement contre des systèmes relativement peu protégés, comme les escroqueries ou les attaques de systèmes sur l'Internet – ne sont en revanche pas de notre ressort. Nous nous intéressons à des systèmes durcis, relativement fermés, qu'il faut protéger d'attaquants de très haut niveau.

En termes de moyens, nous avons essentiellement besoin d'experts très pointus. Nous sommes en très forte croissance : à la fin de l'année 2010, nous disposions de 160 personnes ; nous sommes aujourd'hui 260. La limite à laquelle nous nous heurtons est notre capacité à intégrer et à former les nouvelles recrues de façon efficace. Nous avons la grande chance de disposer des moyens pour les recruter et de pouvoir trouver les bonnes personnes : on dispose en France, aujourd'hui, d'ingénieurs de très haut niveau. Nous espérons dépasser les 400 experts en 2017, ce qui est cohérent avec la montée en puissance de l'ANSSI et des effectifs opérationnels dirigés par le contre-amiral Coustillière.

L'enjeu essentiel est finalement de mener un travail d'architecture intelligent. Nous intervenons lors de la conception des programmes d'armement pour intégrer dès le départ les questions de sécurité, y compris dans les systèmes d'armes, ce qui est assez nouveau dans certains domaines. L'idée est de dessiner pour ces systèmes une architecture d'ensemble qui permettra de les protéger et de les défendre : certaines briques pourront être prises sur étagères, en France ou même à l'étranger, comme des logiciels libres que nous modifions en fonction de nos besoins ; d'autres briques devront être conçues par des industriels de confiance ; d'autres enfin, aujourd'hui assez rares, devront être réalisées en maîtrise d'œuvre étatique, car elles forment le cœur du système. Nous réalisons ainsi nous-même les algorithmes de cryptographie, car sans eux, l'ensemble du système peut s'effondrer. Tout le travail est de concilier un niveau de confiance élevé avec des niveaux d'efficacité, de coût, de délais, compatibles avec les exigences des programmes d'armement.

Mes équipes comptent donc une cinquantaine d'architectes directement au contact des programmes et qui pensent la sécurité à toutes les étapes du développement d'un système. Cela concerne aujourd'hui tout ce qui est développé par la DGA : aucun domaine n'est épargné par les questions de cyberdéfense.

Nous nous appuyons pour cela sur des industriels. La France a aujourd'hui la chance de compter des industries de grande taille et performantes dans ce domaine – c'est rare. Nous sommes également riches en PME dynamiques. Enfin, beaucoup de personnes sont mobilisées à titre personnel dans le domaine de la cyberdéfense – je pense notamment à la réserve citoyenne, qui compte désormais un groupe de réservistes spécialisés en cyberdéfense, dont le coordinateur national est Luc-François Salvador, et dont l'engagement est remarquable.

Le Livre blanc l'a clairement dit : la cyberdéfense est un sujet de souveraineté. Cela ne signifie pas du tout un repli sur soi : cela montre au contraire que nous devons être autonomes et forts pour être crédibles vis-à-vis de nos grands partenaires – ce sont eux qui nous en ont avertis, d'ailleurs. Nous devons être capables, seuls, de protéger nos secrets - étatiques ou industriels – pour être des partenaires avec lesquels on n'aura pas peur d'échanger des informations sensibles et donc pour nouer des alliances.

L'ouverture aux autres se fait ensuite le plus souvent par le biais opérationnel, de préférence de manière bilatérale d'abord, puis avec des partenaires plus nombreux. Évidemment, c'est plus complexe : garder des secrets à vingt-huit, c'est une évidence, n'est pas facile. Mais il est important de mener des opérations multilatérales : les menaces concernent rarement un seul pays. La coopération, au niveau de l'OTAN comme de l'Union européenne, est donc tout à fait essentielle.

En matière de cyberdéfense, il n'est pas inutile d'avoir peur : les dégâts pourraient être considérables. Il faut sonner l'alarme – sans tenir un discours purement anxiogène car le but n'est pas de décourager. Mais il faut vraiment prendre ces menaces au sérieux avant d'être confronté à une catastrophe. Je ne suis pas pessimiste sur ce point : il me semble que beaucoup de gens prennent conscience de l'importance de ces enjeux, notamment en matière de souveraineté.

Je voudrais enfin dire quelques mots de la formation. La France forme aujourd'hui des ingénieurs et des docteurs de très haut niveau. En revanche, aux niveaux inférieurs, nous manquons de filières de formation. Des initiatives sont en cours, notamment dans la région Bretagne. Plus généralement, il faudrait mieux prendre en charge la formation de tous à ce que Patrick Pailloux appelle « l'hygiène informatique ». Les cyberattaques sont rarement totalement automatisées ; le facteur humain est essentiel. Il faut donc adopter des règles élémentaires de sécurité – ne pas utiliser une clé USB dans un ordinateur personnel puis professionnel, ne pas utiliser des moyens professionnels à des fins personnelles et inversement, ne pas utiliser le même mot de passe partout… Ce n'est pas si facile : nous faisons tous des erreurs de sécurité. Ce travail sur l'hygiène informatique est pourtant essentiel ; il faut le mener dans les entreprises, mais aussi dès l'école.

M. Jean-Michel Villaumé. Ces enjeux sont très présents dans le Livre blanc et le seront aussi, je l'espère, dans la LPM. Vous semblez plutôt rassurant sur la cyberdéfense : développez-vous aussi des capacités d'attaque ?

Quels sont nos partenaires pour construire une Europe de la cyberdéfense ?

M. Guillaume Poupard. Le Livre blanc aborde la question des cyberattaques. Ce sont évidemment des sujets classifiés… Ce que je peux vous dire, c'est que les travaux de R&D concernent à la fois la défense et l'attaque : tout ce que l'on peut savoir sur les menaces et les technologies du cyberespace concerne aussi bien l'offensif que le défensif.

L'Europe est un sujet difficile. Nos maîtres d'œuvre industriels m'ont fait remarquer que bien qu'ils soient le plus souvent européens, on leur demande de cloisonner leurs travaux ; chaque pays leur demande de travailler « en silos », avec des équipes qui travaillent côte à côte. Mais si certaines choses relèvent vraiment de la souveraineté, d'autres pourraient utilement être mutualisées, notamment en R&D. Il faut donc certainement renforcer le

dialogue entre les États, mais l'idée de passer par les industriels me paraît très intéressante, d'autant plus s'ils sont demandeurs.

M. Éduardo Rihan Cypel. La cyberdéfense relève à coup sûr de la souveraineté, mais il y a plusieurs niveaux de souveraineté : il faut protéger notre pays, mais aussi nos entreprises et nos libertés individuelles. Vous avez raison : avec des gestes simples, nous pouvons tous mieux protéger nos données personnelles. S'agissant des entreprises – toutes nos grandes entreprises ont, je crois, été attaquées –, quel est votre point de vue ? Faut-il prévoir de nouvelles normes ?

L'affaire Snowden le montre : il faut absolument construire l'Europe de la cyberdéfense, qui pourrait d'ailleurs constituer un moyen d'avancer vers une Europe de la défense. La France a, je crois, fait les choix qu'il fallait avec le Livre blanc, même si ces choix devront être confirmés par la LPM. Mais l'Europe adopte-t-elle une bonne stratégie en matière de cybersécurité et de cyberdéfense ? L'avance française peut-elle favoriser une prise de conscience plus générale ?

Où en sont les entreprises françaises ? Elles sont très dynamiques et en forte croissance, mais sont-elles assez nombreuses ? Sont-elles assez protégées ?

M. Guillaume Poupard. La souveraineté, vous avez raison, concerne aussi les entreprises et les particuliers.

La France vit une situation paradoxale : nous sommes très sensibles à la question des fichiers, et la CNIL a beaucoup travaillé pour éveiller les consciences ; mais nous utilisons énormément les différents réseaux sociaux… Il faut inlassablement rappeler que le droit à l'oubli n'existe pas en matière numérique. Rien n'est gratuit : « quand c'est gratuit, c'est vous le produit. » Il faut donc un effort de formation.

S'agissant des entreprises, la protection du patrimoine scientifique et technique est absolument essentielle.

Les grandes sociétés doivent se donner les moyens de protéger leurs informations. Beaucoup ont aujourd'hui pris conscience de la réalité des problèmes. La LPM comportera sans doute une obligation nouvelle de déclaration d'incident : cela me semble essentiel. Cela permettra aux services de l'État de mieux connaître les menaces et de mieux réagir.

Pour les PME, la situation est très différente : on ne peut pas demander à une PME de dix personnes d'embaucher trois spécialistes en informatique… Il faut donc leur proposer des solutions à leur portée, tant financièrement que techniquement. Aujourd'hui, des offres de *clouds* sécurisés sont lancées en France, d'ailleurs financés en partie par l'État : elles apporteront une solution d'infogérance sûre. Ces offres seront en concurrence avec des offres étrangères, certes très efficaces, mais auxquelles on ne peut pas accorder la même confiance. Des offres nationales, ou européennes, doivent exister.

Le niveau de sécurité de nos entreprises est aujourd'hui insuffisant, l'actualité nous le rappelle régulièrement. On dit en ce domaine qu'il y a les gens qui ont été attaqués et ceux qui ne le savent pas encore… Il faut être très modeste, et le fait qu'aucune alerte ne se déclenche n'est pas rassurant. Il faut « chercher les ennuis » – la plupart de ceux qui ont cherché à détecter des attaques en ont trouvé ! Il y a bien sûr des attaques plus ou moins

graves, allant du site Internet défiguré à la copie de fichiers client, voire au vol de savoir-faire technologique.

S'agissant de l'Europe de la cyberdéfense, elle est aujourd'hui embryonnaire – c'est même un euphémisme. Mais certains pays sont volontaires, comme l'Estonie, qui a été durement attaquée. Nous devons donc trouver des partenaires pour avancer.

Mon sentiment est toutefois que beaucoup de pays ont déjà renoncé, et veulent être protégés plus qu'ils ne veulent prendre en main leur propre cybersécurité. C'est contre cette attitude qu'il faut aller, en leur faisant prendre conscience que beaucoup peut être fait au niveau européen.

M. Christophe Guilloteau. Comment se fait le lien entre les différentes unités qui s'occupent de cyberdéfense ? Nous sommes, je crois, au tout début d'une large prise de conscience sur ce sujet d'avenir : sera-t-il abordé au Conseil européen du mois de décembre ?

M. Guillaume Poupard. Par rapport à notre grand allié d'outre-Atlantique, nous avons la chance d'être petits : la coordination est plus facile… Le contre-amiral Coustillière a réussi à rassembler sous sa direction les équipes opérationnelles de cyberdéfense. Ensuite, il y a l'ANSSI et le pôle que je dirige, dont les experts techniques sont rassemblés à Bruz. Il n'y a donc pas d'éparpillement. De plus, nous soignons beaucoup la qualité humaine des échanges, afin de construire une communauté solidaire où, même si nous serons plus nombreux demain, on saura faire appel à la bonne personne, parce qu'on la connaît. Le CALID et l'ANSSI sont d'ailleurs depuis peu logés dans les mêmes locaux.

La cyberdéfense a été abordée au cours de presque tous les sommets internationaux depuis deux ans : il faut maintenant aller au-delà, et embrayer sur des choses concrètes. C'est plus difficile. Mais cela viendra.

M. Jean-Yves Le Déaut. Monsieur Poupard, vous avez eu raison de souligner qu'il était important de bien maîtriser le numérique, mais encore faut-il qu'existe une bonne gouvernance internationale de ce secteur. La jugez-vous satisfaisante aujourd'hui ? À mon sens, un pays, certes allié et ami, la domine.

Les systèmes sont de plus en plus interconnectés et deviennent donc davantage vulnérables ; dans quels domaines de ces systèmes devons-nous assurer notre souveraineté ? Les logiciels ne feraient-ils pas partie de ce champ stratégique, comme pourrait l'attester, dans le cas des drones, notre volonté de séparer la fourniture des équipements de celle de l'appareil ? Nous pouvons cependant douter de la possibilité d'effectuer une disjonction totale, surtout que nous n'aurons jamais accès aux codes sources de logiciels possédés par plusieurs structures. Or il est tout à fait possible de connaître le réseau et le flux d'informations dès que l'on est connecté à un système informatique.

Vous avez affirmé qu'il était positif que l'ANSSI et les militaires disposent d'un lieu pour se retrouver. Dans mon travail de rédaction du rapport pour avis sur l'environnement et la prospective de la politique de défense, j'éprouve des difficultés à percevoir les liens entre l'académie et le système militaire ; les relations avec l'université et l'institut national de recherche en informatique et en automatique (INRIA) restent insuffisantes. Il est nécessaire de développer la recherche pour pouvoir bien connaître les menaces contre lesquelles nous

devons lutter. Pensez-vous que la liaison avec la recherche civile soit assez développée et comment pourrions-nous la renforcer ?

M. Guillaume Poupard. Il ne m'appartient pas de me prononcer sur la question de la domination de l'Internet, d'autant que la réponse est évidente pour tout le monde.

L'Internet ne constitue pas pour nos applications militaires le support naturel de nos échanges d'informations. Cela serait pourtant pratique et peu cher, mais nous utilisons des satellites et des moyens de radio « propriétaires » – dont le développement s'avère coûteux – car ils nous procurent une confiance dans nos moyens de communication que l'Internet et le GSM ne nous garantissent pas.

Nous ne souhaitons pas maîtriser la conception de l'ensemble des matériels – depuis les transistors jusqu'aux applications logicielles – et, de toute façon, nous ne le pouvons pas. Le travail d'architecture que nous menons vise à déterminer ce qu'il nous faut développer nous-mêmes – ou commander à un partenaire industriel de confiance – pour maîtriser le système que l'on utilise. Nous ne fabriquons plus de microprocesseurs, mais nous produisons des composants électroniques de sécurité et nous intégrons les algorithmes cryptographiques que nous développons dans des puces dont nous surveillons la conception et la réalisation. C'est dans ces domaines que nous concentrons nos besoins de souveraineté ; nous maîtrisons donc certains éléments et nous analysons ce qui nous échappe, afin de disposer de systèmes globalement sécurisés. En outre, ce n'est pas parce que tout n'est pas maîtrisé que le système dans son ensemble ne disposera pas d'un bon niveau de sécurité. L'opinion commune selon laquelle la sécurité d'un système équivaut à celle du plus faible de ses composants s'avère heureusement fausse.

Nous maîtrisons mieux certains logiciels que d'autres, nous ne possédons pas toujours les sources, mais nous n'en avons pas toujours besoin, car leur lecture est complexe et leur lien avec le produit final pas toujours garanti. En revanche, il faut être capable de vérifier la qualité de certaines fonctions de sécurité, ce qui nécessite des compétences et le droit d'y procéder ; le code de propriété intellectuelle n'autorise en effet la rétroconception des logiciels que pour des raisons d'interopérabilité et non de sécurité. Une évolution légale autorisant l'État à effectuer cette rétro-analyse serait ainsi utile.

Nous travaillons au renforcement des liens avec la recherche académique et nous avons déjà développé des relations étroites avec l'INRIA – nous disposons ainsi d'une convention spécifique pour des thèses en cyberdéfense. Des financements de thèses dans des laboratoires tel que celui dit de haute sécurité informatique à Nancy existent par ailleurs, notamment dans le domaine de la virologie. Cela étant, il y a beaucoup de sujets intéressants, un peu moins de chercheurs de haut niveau – car le sujet de la cyberdéfense est récent dans le monde académique – et encore moins de doctorants pouvant ensuite être habilités dans le monde de la cyberdéfense française.

M. Sylvain Berrios. Un référentiel général d'interopérabilité (RGI) et un référentiel général de sécurité (RGS) pour l'ensemble de l'État ont été publiés il y a trois ans, mais il ne me semble pas que l'équivalent existe pour la sphère privée. Quelle est l'implication du ministère de la Défense et de vos services dans ce RGI et ce RGS ? Ceux-ci ont-ils bien été mis en place et respectés par les services de l'État ?

M. Guillaume Poupard. La mise en œuvre du RGS et du RGI dans le ministère de la Défense n'est pas du ressort de mes attributions, mais, si nous n'en appliquons pas systématiquement la lettre, nous en respectons l'esprit. Dans des conditions difficiles comme les opérations extérieures (OPEX), il convient parfois de déroger au RGS pour des raisons d'efficacité ou pour pouvoir travailler en coopération avec d'autres pays de l'OTAN. L'ANSSI est responsable de leur diffusion au sein de la sphère privée, mais nous sommes également concernés, puisque les industriels de défense font partie des opérateurs d'importance vitale (OIV) et que nous devons veiller à ce que les informations dont ils disposent soient protégées ; nous travaillons donc avec eux pour qu'ils mettent en place des méthodes efficaces de protection de leurs données et nous songeons d'ailleurs à élaborer une norme que l'on pourrait développer facilement sur la base du RGS.

M. Sylvain Berrios. Qu'en est-il de l'application du RGS dans les autres départements ministériels ?

M. Guillaume Poupard. Je ne connais pas la réponse à cette question.

Mme Marianne Dubois. Monsieur Poupard, quel est le budget de votre service ?

Les doctorants qui ne souhaitent pas vous rejoindre préfèrent-ils travailler dans le privé pour des raisons financières ?

M. Guillaume Poupard. Nous engageons trois millions d'euros par an pour le soutien aux PME en cyberdéfense. Nous pouvons sûrement faire davantage mais notre objectif est d'utiliser cette ressource financière de manière ciblée pour des acteurs motivés. Ceux-ci sont de plus en plus nombreux et le dispositif devrait par conséquent monter en puissance.

Dans le domaine des études réalisées en amont des projets – principal outil financier à ma disposition –, je suis satisfait des moyens dont je dispose puisqu'ils ont triplé et sont passés de 10 à 30 millions d'euros ; cet effort considérable – même si nous partions d'un niveau relativement faible face aux enjeux – prouve que nous sommes écoutés. Notre principal point de vigilance concerne notre capacité à engager ces crédits de manière efficace et il nous faut développer des idées novatrices avec les bons acteurs académiques et industriels.

Nous développons et achetons également les équipements des forces et la loi de programmation militaire (LPM) devrait fortement augmenter nos moyens en la matière. Notre tâche consiste à nous assurer que des équipements adaptés sont fournis aux utilisateurs.

Nous ne rencontrons pas de difficultés pour recruter des personnes d'excellent niveau et nous avons même attiré des individus dotés d'un CV pouvant rendre envieux n'importe quel géant du numérique. Nous les embauchons à un salaire probablement moins élevé que ce qu'ils pourraient percevoir outre-Atlantique, mais nous leur offrons un environnement de travail de qualité et surtout des sujets passionnants qui ne se retrouvent pas ailleurs. Nous faisons le pari que l'intérêt du métier suffit pour continuer d'attirer de très bons éléments.

Lorsque l'on est diplômé en informatique et que l'on peut trouver du travail en quelques jours, débuter une thèse exige de posséder un fort intérêt pour la recherche académique. Nous devons nourrir cette motivation en mettant en avant, là encore, l'intérêt du

travail, la réévaluation des bourses de thèses – pour nécessaire qu'elle soit – n'étant qu'une question secondaire.

Mme la présidente Patricia Adam. Nous vous remercions, Monsieur Poupard, de cet exposé complet et clair. Nous recevrons M. Patrick Pailloux, directeur général de l'ANSSI, mardi 16 juillet.

La séance est levée à dix-sept heures trente.

*

* *

Membres présents ou excusés

Présents. - Mme Patricia Adam, M. Sylvain Berrios, M. Jean-Jacques Bridey, M. Jean-Louis Costes, Mme Marianne Dubois, M. Yves Fromion, Mme Geneviève Gosselin-Fleury, M. Christophe Guilloteau, M. Jean-Yves Le Déaut, Mme Émilienne Poumirol, M. Eduardo Rihan Cypel, M. Gwendal Rouillard, M. Jean-Michel Villaumé, M. Philippe Vitel, Mme Paola Zanetti

Excusés. - M. Ibrahim Aboubacar, M. Claude Bartolone, M. Philippe Briand, M. Jean-Jacques Candelier, M. Laurent Cathala, M. Sauveur Gandolfi-Scheit, M. Serge Grouard, Mme Edith Gueugneau, M. Éric Jalton, M. Frédéric Lefebvre, M. Bruno Le Roux, M. Maurice Leroy, M. François de Rugy