ASSEMBLÉE NATIONALE

XIVe LÉGISLATURE

Compte rendu

Commission de la défense nationale et des forces armées

Mardi
28 juin 2016
Séance de 17 heures

Compte rendu n° 61

SESSION ORDINAIRE DE **2015-2016**

Présidence de Mme Patricia Adam, *présidente*

ASSEMBLÉE NATIONALE

La séance est ouverte à dix-sept heures.

Mme la présidente Patricia Adam. Nous accueillons l'amiral Arnaud Coustillière, directeur de projet chargé de la coordination générale des actions du ministère de la Défense dans le domaine de la cyberdéfense.

Nous vous avons entendu il y a trois ans, amiral, à l'occasion de la préparation de la loi de programmation militaire (LPM). La cyberdéfense est devenue une préoccupation première du ministère de la Défense et de notre commission. Même si le ministre s'est déjà exprimé sur la question, nous allons entrer un peu plus dans le détail pour savoir où nous en sommes et pour savoir ce qui reste à faire.

Amiral Arnaud Coustillière, directeur de projet chargé de la coordination générale des actions du ministère de la Défense dans le domaine de la cyberdéfense. J'ai commencé à travailler sur le dossier de la cyberdéfense en 2009, au moment de la sortie du Livre blanc sur la défense et la sécurité nationale pour 2008-2013, avant d'être nommé le premier officier général à la cyberdéfense en juillet 2011 – j'entame donc ma sixième année dans mes fonctions. Depuis, notre capacité de cyberdéfense – la lutte informatique défensive – et notre capacité offensive se sont considérablement amplifiées. L'État a ainsi fourni un très sensible effort pour rattraper son retard en la matière, si bien que, sans donner dans le triomphalisme, nous faisons désormais partie, avec les États-Unis et le Royaume-Uni, du club des trois nations occidentales dotées de telles capacités, et avec la volonté de s'en servir – de fait nous sommes en guerre contre Daech notamment.

Ma responsabilité porte sur le volet militaire des opérations de cyberdéfense. Je travaille de façon très étroite avec mon camarade Guillaume Poupard, successeur de Patrick Pailloux, en 2014, à la tête de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) – qui s'occupe de la cyberdéfense dans le domaine civil, en particulier de la cyberdéfense des grands organismes liés aux secteurs d'intérêts vitaux de l'État, et de la politique de régulation qui est en train de se mettre en place.

La cyberdéfense française se distingue de celle des pays anglo-saxons dans ses rapports avec le monde du renseignement. Le modèle anglo-saxon de la cyberdéfense est beaucoup plus intégré : le *United States Cyber Command* (USCYBERCOM) et la *National Security Agency* (NSA) américains sont en effet très proches, de même que, au Royaume-Uni, le renseignement technique, le *Government Communications Headquarters* (GCHQ), assure également la cyberdéfense de la société civile. En France, nous avons choisi, à l'inverse, une séparation nette entre ce qui relève des interceptions ou du renseignement dans l'espace numérique, qui est du domaine de compétence des services de renseignement, et ce qui ressort de la lutte informatique défensive, de la défense de la Nation, des données personnelles et des données des entreprises, qui ressortit aux acteurs du volet défensif de la cyberdéfense et est confié d'un côté à l'ANSSI et de l'autre à la chaîne de commandement que je dirige au ministère de la Défense – cela dans un cadre juridique particulier défini par les articles 21, 22 et 23 de la loi de programmation militaire, qui couvrent en particulier les opérateurs d'importance vitale (OIV).

Tout le fonctionnement des institutions, des infrastructures nationales repose désormais, vous le savez, sur l'informatique. C'est également le cas, dans le domaine économique, pour nos concurrents, y compris Occidentaux, qui sont donc prêts à utiliser

l'espionnage informatique – et il en va de même, j'imagine, dans le monde politique. Dans l'univers stratégique et militaire, nos ennemis sont identifiés, au premier rang desquels se trouve le terrorisme islamiste. Les capacités d'action de nos adversaires sont plus ou moins importantes et représentent une menace directe ou indirecte contre nos capacités militaires – aussi devons-nous être capables de déployer nos forces face à tout type d'attaque informatique.

Nous devons faire face au sein de l'espace européen à des actions informatiques sophistiquées que l'on attribue plus ou moins à des groupes de *hackers* d'obédience mafieuse – on cite souvent dans les rapports des industriels de la cybersécurité, le groupe APT28 qu'on retrouve dans des attaques contre le parti démocrate américain, contre TV5, contre le *Bundestag* allemand et récemment contre la Suisse. On retrouve ces groupes mafieux versés dans la cybercriminalité dans des attaques à visée plus stratégique. Ainsi, le piratage de TV5 a été revendiqué par un groupe prétendument islamique dénommé *Cyber Caliphate*, qu'aujourd'hui les sources averties stigmatisent comme faux nez du groupe APT28. Les acteurs de l'espace numérique sont très divers et il reste très difficile d'en cibler l'origine. L'espace numérique tend à gommer les frontières, les nationalités, les références.

Cela signifie pour nous, militaires, un changement d'époque, une révolution. Depuis les années 1950, nous avons numérisé, par nos systèmes d'information, l'ensemble des processus, les espaces de bataille, ce qui nous a conféré un avantage militaire important sur nos ennemis. Puis, comme dans la société civile, il y a eu un revirement : le numérique s'impose désormais à nos vies et avec son propre tempo. Pour nous, le numérique est désormais considéré comme un nouvel espace de combat, à côté de l'espace terrestre ou de l'espace aérien. Or, dans ce nouvel espace, comme dans les autres, on ne maîtrise pas tout : quand on numérise un processus, on considère qu'on le maîtrise ; mais quand on se déploie dans un espace numérique, avec de très nombreux acteurs, sur les réseaux sociaux, qui vous observent, avec de très nombreuses technologies à intégrer dans nos systèmes d'armes, j'y insiste : on ne maîtrise pas tout – pas plus qu'on ne maîtrise le fond sous-marin ou un cumulonimbus qu'on traverse en avion. Or l'espace numérique abrite un certain nombre d'éléments nocifs qui agissent contre les intérêts de la France et qu'il va falloir apprendre à combattre. C'est à ce changement de paradigme que l'on assiste actuellement dans les armées et qui explique que l'on parle de nouvelle composante, l'Organisation du traité de l'Atlantique nord (OTAN) reconnaissant il y a peu le numérique comme un nouvel espace de combat.

Le Livre blanc sur la défense et la sécurité nationale de 2013 a défini des ambitions et la loi de programmation militaire prévue des moyens. Nous avons, au sein du ministère de la Défense, conclu un « Pacte Défense Cyber 2014-2016 ». Ce plan stratégique de six grands axes et 50 mesures – en matière de réorganisation, de financement, de recrutement… – est quasiment achevé. Il reste néanmoins beaucoup à accomplir dans le domaine des ressources humaines : une capacité en matière de cyberdéfense, c'est avant tout une capacité humaine. Ceci peut paraître paradoxal, mais s'il est vrai que la cyberdéfense suppose l'emploi d'une technologie de pointe, dans une perspective de combat – qu'il s'agisse de se défendre ou d'attaquer –, les compétences humaines sont indispensables moins d'un point de vue quantitatif que qualitatif. Vous pouvez par exemple vous doter de n'importe quelle technologie, si vous ne disposez pas pour l'utiliser des bons personnels pour régler les bons paramètres et pour comprendre le contexte, cette technologie ne sert à rien puisque le but de l'attaquant sera précisément de la contourner en en trouvant les failles ou en en modifiant les réglages.

Nous avons à cette fin créé des postes – quelque 1 500 sont prévus pour la période 2013-2019 et correspondant à tous les profils du ministère de la Défense. Le véritable enjeu est de savoir comment fidéliser ces personnels, quel parcours de carrière leur proposer, quelle doit être la part des experts pointus par rapport à la part des experts opérationnels, quelle doit être la part des civils… Voilà le chantier qui nous attend.

Le « Pacte Défense Cyber » déjà mentionné définit une stratégie de concentration des ressources humaines sur deux lieux principaux : la région parisienne, bien sûr, puisque c'est là que nous avons une série de centres d'opérations, ce qui est également le cas des grands services de renseignement ; et, fin 2011-début 2012, nous avons choisi la région Bretagne parce que s'y trouvent, d'une part, le centre d'expertise de la DGA-MI (direction générale de l'armement-maîtrise de l'information), destiné à devenir l'arsenal français en matière de cyberdéfense et, d'autre part, le creuset de la formation interarmées à l'école des transmissions situé à Cesson-Sévigné.

Dès sa prise de fonctions, le ministre de la Défense a décidé d'accélérer le processus tout en donnant une dimension certaine au pôle d'excellence cyber (PEC) de Bretagne afin qu'il concentre nos ressources humaines. Il s'agit de la création de plusieurs emplois autour de Rennes et, plus largement, dans la région Bretagne. Quatre pôles de compétence vont être institués : le premier, très technologique, à Bruz, où se trouve déjà la DGA-MI, et où un bâtiment d'expertise cyber de haute sécurité est en construction – c'est là que se développeront les activités en matière de recherche et développement ; au quartier militaire de La Maltière, où nous concentrerons une compagnie d'expérimentation de guerre électronique, une compagnie de protection de cyberdéfense et une partie de notre centre de défense informatique, travailleront 350 personnes ; les deux derniers pôles seront consacrés à la formation, l'un à Coëtquidan, l'autre à Cesson-Sévigné, avec un certain nombre d'écoles civiles. Le pôle d'excellence Bretagne comporte également un volet civil, un partenariat étroit ayant été signé avec la région.

Par ailleurs, la loi de programmation militaire prévoit un programme d'armement de plus de 350 millions d'euros consacrés au volet défensif – les chiffres du volet offensif sont classifiés mais peuvent être obtenus dans un autre cadre.

Depuis l'été 2015, nous avons déménagé au site de Balard. Le commandement de cyberdéfense est désormais en route, bien qu'encore réduit et il est pleinement intégré au pôle opérationnel du site. Je dispose ainsi d'une sorte d'état-major opératif au même endroit que l'état-major opératif du commandement des opérations spéciales (COS), que les plateaux de la direction du renseignement militaire (DRM), que les états-majors qui conduisent les opérations par zones – éléments avec lesquels nous pouvons ainsi travailler en totale synergie. Il s'agit bien pour nous d'intégrer le combat dans l'espace numérique avec les autres formes de combat, autrement dit, il s'agit de savoir comment gérer un milieu supplémentaire dans une approche globale entre les capacités de ciblage cinétique – à savoir le largage de bombes – et les capacités de ciblage numérique – à savoir l'engagement d'un ennemi dans l'espace numérique –, en fonction d'une logique milieu menant-milieu concourant, et selon laquelle nous nous appuyons les uns et les autres. Voilà les travaux que nous menons, que nous apprenons à conduire, qu'ils aient une vocation défensive en complément de nos plans CUIRASSE de protection ou de soutien des opérations extérieures (OPEX).

En matière de coopération internationale, nous entretenons des relations très étroites avec nos partenaires britanniques et avec les Américains. Nous avons également des rapports particuliers avec plusieurs pays européens comme l'Estonie – nation phare en matière de cyberdéfense et pourvue d'excellents laboratoires : nous disposons d'ailleurs d'un officier au centre d'excellence de Tallinn et nous en enverrons un second cette année pour prendre la tête de l'entraînement. En effet, nous croyons beaucoup à l'entraînement à distance tel que le pratique le centre d'excellence de l'OTAN. Lors de ces entraînements, on simule des attaques en rouge sur un grand réseau sur lequel chaque pays peut se connecter à partir de son propre centre de cyberdéfense. Nous y avons participé pour la troisième fois cette année. Nous sommes en train de mettre en place ce système d'entraînement pour nos propres armées, le cœur de ce réseau de simulation devant se situer à l'école de Saint-Cyr Coëtquidan.

Lors du sommet de Varsovie, l'OTAN va consacrer un effort supplémentaire à la cyberdéfense et reconnaître qu'elle est un domaine opérationnel à part entière. Au sein de l'Union européenne, c'est plutôt l'ANSSI donc le secteur civil qui est en pointe. Enfin, nous entretenons des relations bilatérales avec une quinzaine de nations.

Le développement d'une réserve opérationnelle de cyberdéfense est le dernier projet d'envergure en date. La phase de recrutement a déjà commencé. Nous en avons eu l'idée en 2011 avec Patrick Pailloux, puis nous l'avons suggérée dans le cadre des travaux sur le Livre blanc, enfin nous l'avons étudiée avec nos camarades de la gendarmerie, l'ANSSI et certains services du ministère de l'Intérieur. Et, une fois le projet mûr, nous en avons demandé l'inscription dans l'actualisation de la loi de programmation militaire. Les derniers textes datant de la fin mai 2016, nous avons désormais les moyens de le réaliser et avons d'ores et déjà créé la structure administrative pour pouvoir recruter. L'objectif est de mettre en place une réserve à même d'intervenir au profit du ministère de la Défense ou à celui de l'ANSSI, par réquisition, ou au profit des forces militaires selon les procédures en vigueur. Il s'agit de pouvoir mobiliser immédiatement des spécialistes pour intervenir et des personnels moins experts pour la phase de reconstruction de réseau. À cet effet, des protocoles seront passés par le ministère de la Défense avec les directeurs d'un certain nombre de grandes sociétés d'informatique qui nous auront rejoints dans le cadre du pôle d'excellence Bretagne. Nous entendons disposer d'un réservoir de forces d'un volume important : 400 postes de réservistes opérationnels et 4 000 postes de réservistes citoyens recrutés dans les écoles par le biais d'exercices de préparation militaire cyber – que nous sommes capables, quand nous les activons, de basculer en réservistes opérationnels du ministère de la Défense dans un délai d'une quinzaine de jours, délai totalement compatible avec le temps que prend l'analyse d'une intervention, la conception d'un plan de reprise et la reconstruction d'un réseau puisque, généralement, la phase d'observation d'une attaque dure plusieurs semaines.

Mme Geneviève Gosselin-Fleury. Un exercice interarmées DEFNET a été effectué en mars 2016 sur plusieurs sites militaires du territoire national et sur cinq bâtiments de surface de la marine nationale. Selon mes informations, 200 étudiants d'établissements de l'enseignement supérieur, cinq parisiens et sept de Bretagne, y ont participé dans le cadre de l'expérimentation de la réserve cyberdéfense. Quel bilan tirez-vous de cet exercice quant à la participation de ladite réserve ?

M. Gilbert Le Bris. Merci amiral pour toutes vos précisions qui nous ont fait quelque peu sortir du « cyberflou », même s'il reste bien entendu des zones difficilement compréhensibles pour nous.

Pourriez-vous nous donner, à titre d'illustration, un exemple d'incident ou d'accident ?

Ensuite, vous intervenez également pour la réalisation de réseaux aussi complexes que le système d'information des armées (SIA), *via* le groupe Sopra Steria. Avez-vous les moyens d'agir en amont et de contrôler, éventuellement, ce qui se fait en la matière ?

Enfin, vous avez évoqué l'OTAN avec, en particulier, le pôle d'excellence de Tallinn. Les différents pays de l'Alliance cherchent-ils à renforcer la cohérence entre eux ? Et, dans l'affirmative, cette recherche nous a-t-elle conduits à modifier nos propres standards, nos modes d'intervention ?

M. Jean-Jacques Candelier. Merci, amiral, pour les informations que vous nous avez apportées. Je commencerai par une question délicate : pourquoi avons-nous étouffé – c'est bien le terme – l'affaire de la NSA (*National Security Agency*) dévoilée par M. Snowden et pourquoi le gouvernement français passe-t-il des accords avec la société Cisco, bras armé de la même NSA ?

Ensuite, l'amiral Sanguinetti, alors major général de la marine sous Georges Pompidou, ce qui ne nous rajeunit pas, dénonçait notre dépendance coupable, en matière de chiffrement, vis-à-vis de l'OTAN. En quoi les choses ont-elles changé depuis notre réintégration du commandement intégré de l'OTAN ?

Par ailleurs, sommes-nous vraiment à l'abri d'une cyberguerre, avec piratage des systèmes de commande et de contrôle des armes nucléaires, le lancement et la mise à feu de ces dernières pouvant causer une catastrophe sans précédent dans l'histoire de l'humanité ?

Enfin, de la même manière, *quid* d'une prise de contrôle de nos drones dans l'hypothèse d'une faille de notre cyberdéfense ?

Amiral Arnaud Coustillière. Pour répondre aux deux dernières questions de M. Candelier, mener des attaques informatiques contre nos systèmes protégés n'est pas si simple : il s'agit de réelles opérations militaires qui nécessitent le recueil de très nombreux renseignements en amont, de mener des actions préalables. Grâce au chiffrement souverain, à la segmentation des réseaux, à la séparation et à la duplication des réseaux, on peut estimer que même une nation disposant de fortes capacités ne serait pas capable d'une prise de contrôle telle que celle que vous évoquez et qu'il lui serait plus simple de parvenir à ses fins par des moyens cinétiques ou par le biais d'une action humaine. Pour chacun des systèmes que nous développons, nous tenons compte du critère d'exposition à une attaque : plus le système est éloigné d'internet, plus une attaque est compliquée à mener.

Il faut bien se rendre compte que l'introduction d'une dimension supplémentaire, l'espace numérique, tend à amplifier tout ce que vous pouviez déjà imaginer dans les autres espaces. Certes, un romancier imaginera un type qui, depuis son laboratoire, prendra à distance le contrôle d'un drone mais, personnellement, je n'y crois pas : des *gaps* (séparations physiques) ont été mis en place – du moins dans le domaine militaire. Et si nous réalisons d'énormes investissements en matière de cyberdéfense, c'est bien pour nous prémunir de telles éventualités, et avoir un coup d'avance.

Vous avez par ailleurs posé une excellente question, Monsieur Candelier, sur la place des grandes entreprises comme Cisco ou Microsoft. Nous n'allons pas refaire le monde : il avance et demain, Cisco ou Microsoft et leurs concurrents sont Huawei ou autres… L'Europe a raté son tournant numérique et le plan informatique qu'elle avait élaboré dans les années 1970 a échoué. Le monde avance, et les usages s'imposent à vous : vous n'allez pas arrêter Facebook ni Twitter. Quand on observe la façon dont certains pays manipulent tous les réseaux sociaux, on se rend bien compte que ces usages font partie intégrante de la vie d'une nation.

C'est ce que signifie l'idée selon laquelle nous avons basculé d'une numérisation de systèmes vers l'espace numérique. Nous vivons dans cet espace et c'est un fait. Il va donc falloir que nous utilisions des technologies de provenances diverses, de la technologie non maîtrisée – plus personne ne fabrique de composants élémentaires en France, aujourd'hui ; aussi, sauf cas très particulier, nous allons les acheter chez un fabricant tiers. Or, dans 80 % des cas, ce fabricant est asiatique. Nous devons donc apprendre à constituer un ensemble de sous-systèmes dont les composants ne nous inspirent pas la moindre confiance, et à entourer ces sous-systèmes de points de mesure pour être sûrs que ce qui y entre et ce qui en sort ne renseigne ni nos concurrents ni nos adversaires. Et, à cette fin, la direction générale de l'armement dépense beaucoup d'argent. Quand on lance un appel d'offres pour acheter des routeurs, on trouve, sur le marché, Cisco, IBM… L'industrie européenne, en matière de technologie des réseaux, n'existe quasiment plus, hormis, sans doute, Alcatel qui est en train d'être repris par Nokia, mais je m'éloigne de mes domaines de compétence.

L'affaire Snowden n'entre pas dans mon périmètre et je regrette de devoir botter en touche : je ne dirige pas un service de renseignement. Cette affaire a éclaté aux États-Unis parce qu'il s'y trouve toujours quelqu'un pour donner l'alerte. Prenez le système russe, vous y trouverez un équivalent. L'internet chinois, l'internet iranien sont complètement contrôlés. L'Algérie vient de débrancher ses réseaux sociaux pour éviter la tricherie au baccalauréat. De nombreuses nations essaient ainsi de réguler cet espace et les réseaux sociaux. L'affaire Snowden en fait partie et je ne suis pas naïf. C'est pourquoi, au début de mon propos, je distinguais les concurrents des ennemis. Or dans le monde économique, nous avons des concurrents y compris parmi nos proches alliés.

Dans l'OTAN nous n'avons jamais quitté la structure politique et militaire de l'Alliance. Nous disposons d'équipements de chiffrement nationaux et nous maîtrisons complètement la cryptographie qui, je le rappelle, repose sur l'école de mathématiques française ; or si l'on fragilise cette dernière, d'ici à vingt ans il n'y aura plus de cryptographie nationale. Pour l'heure, la cryptographie est entretenue par l'État au sein de la DGA-MI, ses équipements étant fabriqués par nos industriels. Elle relève donc du domaine régalien. Il n'existe pas de « chiffre OTAN » pour nos réseaux nationaux.

On m'a par ailleurs demandé de citer un exemple d'incident. Typiquement, à partir de marqueurs d'attaques, nous recherchons sur toutes les traces de navigation du ministère de la Défense si, par hasard, certaines ne ressortent pas. Nous avons des marqueurs provenant du monde du renseignement. Un marqueur peut être un petit bout de bit – 3, 4, 0 et 1 dans un ordre qui peut être un peu différent – qui est la marque d'un certain type d'attaque tel qu'il a déjà été repéré à différents endroits. On récupère dès lors les *logs* – la somme du trafic réalisé par un ordinateur ou un serveur, à savoir des tétra-données –, le travail des acteurs de la cyberdéfense étant de rassembler les signaux faibles ainsi repérés et d'analyser un phénomène

paraissant ainsi bizarre. Les recherches peuvent mener, par exemple, sur une campagne de *mails* ciblant 1 % des adresses du réseau internet de l'armée de l'air. Nous nous sommes alors rendu compte que 350 de ces courriels avaient corrompu quatre machines sans toutefois que le logiciel n'aille plus loin. C'est un groupe mafieux qui a mené cette opération.

Autre exemple : des patrouilles de cyberdéfense se « promènent » sur nos réseaux avec des outils d'opérateur pour déceler des dysfonctionnements, de mauvaises configurations que nous analysons à distance en prenant des empreintes afin, toujours, de repérer des signaux faibles. Nous comparons ainsi toutes les configurations de 5 000, 10 000 voire 20 000 postes de travail pour tâcher de repérer des anomalies. Généralement, un véritable attaquant va entrer en se faisant le plus discret possible et il nous revient d'aller le chercher par le biais de ces patrouilles – les Américains parlent de *hunting*. Il peut s'agir du *hacker* du coin qui pénètre notre réseau, nos sites ouverts sur internet, d'où nous devons le faire sortir. Si les membres de votre commission souhaitent effectuer une visite du centre d'analyse de lutte informatique défensive (CALID) pour connaître plus de détails, je l'organiserai avec grand plaisir.

En ce qui concerne les programmes d'armements, je ne participe pas à leur conception en amont. Il existe cependant, en amont, une fiche d'expression des besoins en matière de sécurité, sous la responsabilité des officiers de cohérence opérationnelle. En revanche, la DGA-MI désigne un architecte qui va suivre le processus. Je fais pour ma part partie de la commission d'homologation de sécurité et je dois signer le document attestant que je prends en charge le système dans mon dispositif de défense – en connaissant ses failles de sécurité. Je suis donc acteur et non concepteur.

Le centre d'excellence de Tallinn fonctionne remarquablement bien. Il a commencé par mener de nombreuses études juridiques pour aujourd'hui concentrer ses activités sur l'entraînement. Il devient donc le bras armé de l'OTAN en la matière, étant entendu que l'Alliance, censée développer des capacités défensives de cyberdéfense, n'a pas de capacités offensives, les nations membres refusant de lui en donner. La mission de l'OTAN consiste par conséquent à donner un espace d'interopérabilité pour que les nations puissent augmenter leurs capacités et à défendre les systèmes propres de l'OTAN, qui correspondent à ceux d'une grosse PME. L'avantage de ce système est que les nations peuvent se retrouver, discuter et se mettre d'accord sur des processus. Le centre d'entraînement de Tallinn est de ce point de vue excellent, j'y insiste, puisqu'il nous offre une plateforme de processus agréés par l'OTAN et sur lesquels chaque nation vient se « *plugger* ». L'Alliance nous donne des scénarios de très bon niveau, ce qui est très valorisant pour nos équipes ; ainsi l'exercice *Locked Shields* auquel nous nous sommes livrés pour la troisième année consécutive était de très haut niveau. Nous pouvons à cette occasion nous mesurer aux autres nations. Reste que nous n'en sommes pas encore au stade de l'interopérabilité : nous n'irons pas révéler à une autre nation quelles sont nos pratiques, quels sont nos outils spécifiques ; aussi nous tenons-nous côte à côte mais pas ensemble. L'intégration, en matière numérique, n'est pas la même que celle concernant les autres espaces. On peut l'illustrer en évoquant deux bateaux qui avancent de conserve mais dont les équipages ne sont pas interchangeables. Et encore faudrait-il que nous ayons quelque chose de commun à défendre ; or chaque nation défend ses propres réseaux et n'admettrait pas qu'une autre y installe des capteurs.

J'en viens à DEFNET, exercice annuel d'entraînement de la chaîne de cyberdéfense : le commandement opérationnel s'emploie à coordonner différents incidents à divers endroits ; c'est pourquoi sont impliquées la marine, l'armée de l'air et l'armée de terre avec des

scénarios qui leur appartient de définir. Depuis trois ans, nous testons les dispositifs de la réserve cyberdéfense avec les étudiants d'un certain nombre d'écoles partenaires et nous définissons avec eux ce que l'État peut leur apporter. Nous nous sommes ainsi rendu compte que les scénarios intéressaient beaucoup leurs professeurs. Nous avons commencé par les écoles de la région parisienne et celles de la région Bretagne parce que c'était plus simple pour nous, mais dès le DEFNET 2017 nous travaillerons avec des écoles toulousaines et bordelaises et, en 2018, nous remonterons vers Lyon et vers l'est – le tout étant corrélé avec le plan de déploiement de la réserve de cyberdéfense. Nous organiserons par ailleurs une semaine de la cybersécurité à la mi-octobre, un « hackathon » auquel participeront plusieurs écoles.

M. Jean-Michel Villaumé. Quel type de cybermenaces vous inquiète-t-il le plus pour la sécurité des intérêts français ? Je pense notamment aux entreprises stratégiques. J'ai lu un entretien que vous avez accordé en 2015 dans lequel vous estimiez que le cyberterrorisme d'un groupe comme Daech n'était pas trop inquiétant dans la mesure où cette organisation se limitait à la propagande sans avoir l'expérience, les personnels, les moyens techniques de nous menacer réellement. Avez-vous évolué sur le sujet, autrement dit, est-ce que Daech est plus inquiétante aujourd'hui qu'en 2015 ?

M. Philippe Nauche. Merci amiral, pour vos précisions. Manifestement, le cyberespace est devenu un milieu à part entière en matière de défense. Dès lors, cela aurait-il du sens de l'individualiser en tant qu'armée, de la même manière qu'il y a une armée de terre, une armée de l'air, une marine ? Ou bien une telle nouvelle armée serait-elle un gadget ? Les OPEX sont souvent réalisées sur le mode interarmées, au moyen de groupements tactiques interarmes (GTIA), aussi le fait de disposer d'une armée dédiée ne favoriserait-il pas une telle intégration ?

Ensuite, y a-t-il, selon vous, des industries de souveraineté qu'il faudrait promouvoir pour améliorer notre cybersécurité ?

Enfin, le pôle d'excellence Bretagne est-il complet en matière de coopération entre le ministère de la Défense et votre service ?

M. Gilbert Le Bris. Bien sûr ! *(Sourires.)*

M. Gwendal Rouillard. Quel regard portez-vous, amiral, sur la capacité de la France, de nos entreprises à produire les technologies nouvelles dont nous avons besoin, en particulier pour nous protéger ?

Ensuite, la France a des coopérations militaires multiples. Dans le cadre de nos futures coopérations militaires ou de celles que nous allons renouveler, quelle est la place de la cyberdéfense ?

M. Christophe Guilloteau. Notre collègue Le Bris dit être sorti, grâce à votre intervention, amiral, du « cyberflou », mais qu'en est-il du « cybersous » ? Après la parution du Livre blanc, on avait parlé d'un milliard d'euros…

Amiral Arnaud Coustillière. Le milliard d'euros auquel vous faites allusion inclut ce qu'on appelle, dans notre jargon, le titre 2. Il s'agissait d'atteindre ainsi un niveau symbolique.

M. Christophe Guilloteau. Cette enveloppe a dû augmenter un peu.

Amiral Arnaud Coustillière. En effet.

On connaît parfaitement bien le coût des programmes d'armement pour le volet défensif : 350 millions d'euros pour 2013-2019.

Le coût de la capacité offensive est quant à lui lié pour un tiers aux ressources humaines, un petit tiers aux coûts de fonctionnement et d'investissements et un gros tiers aux coûts d'infrastructures – pour loger le personnel et construire des laboratoires.

Aussi étonnant que cela paraisse, le volet infrastructures de la capacité informatique coûte très cher.

M. Christophe Guilloteau. Et tout cela est vite obsolète !

Amiral Arnaud Coustillière. Non, je n'évoque ici que l'infrastructure, à savoir la « boîte », le béton… Si pour fabriquer un réseau intranet entreprise il faut compter des centaines de millions d'euros, l'établissement d'un gros programme de surveillance d'un grand réseau coûtera de 10 à 20 millions d'euros. Les programmes spécifiques cyber ne sont pas particulièrement chers, toutes proportions gardées, par rapport à la qualité de la ressource humaine et à la prestation de service offerte. Une salle de supervision, en équipements informatiques, ne représente pas un investissement énorme – il n'a rien à voir avec le prix d'un Rafale ou le prix de la salle de contrôle de tir d'une fusée Ariane – ; en revanche, les experts qui se trouvent derrière les écrans coûtent cher.

Pour ce qui est des coopérations militaires renouvelées, en matière de cyberdéfense, il faut avoir des compétences techniques et la volonté de s'en servir. On retrouve, dans ces coopérations, les mêmes partenaires que sur les théâtres d'opération.

J'en viens à la question de la cyberarmée. Les armées ni même l'État ne peuvent échapper à l'introduction du numérique. L'espace numérique irrigue très profondément tous les systèmes, tous les bateaux, tous les avions et jusqu'au fantassin qui a des équipements et des liaisons intégrés (FÉLIN), qui a une adresse IP sur lui. Le véhicule de combat de l'avant sera, dans quelques années, de même que la voiture intelligente, une sorte de système androïd, si je puis dire, auquel on aura mis des roues et qu'on aura pourvu d'une certaine intelligence. Ensuite, le domaine des systèmes d'information va nous permettre d'exploiter ce milieu numérique et, au-dessus, nous avons les combattants – ceux qui se défendent et ceux qui attaquent –, voilà ce qu'est la cyber.

Cette évolution justifie-t-elle la création d'une armée distincte des autres, avec ses logiques propres ? Je doute que ce soit une bonne solution à court terme parce que nous risquons alors de perdre en cohérence en sortant les spécialistes des différentes armées, en provoquant une telle cassure. Reste que je n'ai pas de boule de cristal, pas plus que le militaire de 1912 qu'on aurait interrogé sur l'avenir éventuel de l'arme aérienne. Le sujet mérite cependant d'être posé et d'être analysé par ceux qui réfléchissent aux évolutions des armées. En revanche, ce que je sais, c'est que le temps s'accélère et que, du côté américain, où l'on a en général toujours un peu d'avance, on n'envisage pas une armée cyber, chacune des composantes s'appropriant au contraire la cyberdéfense. Il me semble qu'il s'agisse de la meilleure voie, à condition que chacune des armées joue le jeu et consacre la ressource

humaine nécessaire aux biens communs interarmées. Si les armées ne fournissent pas les compétences dont nous avons besoin il y aura en effet un problème.

La création éventuelle d'une armée numérique est une question complexe mais qui est à traiter. Ce n'est toutefois pas un problème uniquement de cyber.

M. Villaumé m'a interrogé sur Daech. En Syrie, l'organisation dispose, en matière informatique, de gens particulièrement compétents mais qui servent principalement sa propagande, garantissant que son système d'information fonctionne bien – puisqu'il est vital pour elle, pour afficher sa puissance, de montrer qu'elle existe bien plus que ce n'est le cas en réalité – et qui assurent ses flux logistiques, qu'il s'agisse de son approvisionnement, de ses trafics en tous genres ou de son financement. En parallèle, des groupes se référant à Daech, sortes de franchisés, comme *Cyber Caliphate* et autres, vont mener des attaques informatiques de bas niveau – effacements, vols de données déjà en ligne – et vont faire du bruit. Ils n'ont en tout cas pas actuellement la possibilité de faire très mal mais ils évoluent. En revanche, ils sont capables de créer de l'anxiété – il est par exemple perturbant pour une mairie de voir la page d'accueil de son site remplacée par une représentation du drapeau de Daech. Ces groupes sont sans doute pour certains francophones et se trouvent donc dans les pays du pourtour méditerranéen ou aux confins de l'Europe. Par ailleurs, dans la zone moyen-orientale, vous avez des groupes beaucoup plus performants mais qui concentrent leurs actions plutôt sur Israël, sans trop intervenir dans notre zone.

Pour ce qui concerne la capacité des entreprises, la France dispose de PME très innovantes mais de trop petite taille ; aussi le vrai enjeu est-il de savoir de quelle manière elles peuvent s'adosser aux quelques grands groupes comme Airbus, Thales, SOGETI, Sopra Steria, ATOS, de manière à ne pas « tuer » leur innovation – souvent les patrons de ces PME sont de fortes personnalités et intégrer une grande structure est souvent délicat – et afin que soit préservé leur dynamisme. Si l'on veut avoir un tissu industriel, l'État a agi comme il convenait en instaurant, par exemple, le programme d'investissements d'avenir (PIA). En matière d'aide à l'innovation, les PME peuvent trouver des financements pour peu que leurs projets tiennent la route. Le ministère de la Défense via la DGA et les projets RAPID en est un acteur important. Je fais pour ma part partie de l'équipe d'encadrement du concours « Innovation 2030 » et, parmi les dossiers qui nous ont été présentés, certains étaient très intéressants. Si le financement initial ne pose pas de problème, on note un souci de pérennisation ; c'est pourquoi les régions ont à mon sens un rôle particulier à jouer. C'est le défi relevé par la région Bretagne et le pôle d'excellence cyber, constituant ainsi un terreau favorable pour certaines PME, étant entendu qu'il ne s'agit pas de rayonner pour la Bretagne mais à partir de la Bretagne. Le ministère de la Défense travaille également avec Bordeaux et Toulouse – l'*Aerospace Valley* fonctionne.

M. Philippe Nauche. Ma question portait sur les industries de souveraineté dont vous pensez qu'elles sont absentes et qu'il faudrait stimuler *via* des moyens régionaux.

Amiral Arnaud Coustillière. Ce qui revient à savoir comment sécuriser un système dont on n'est pas sûr. On ne va bien sûr pas remplacer Cisco ou Microsoft ; en revanche, on installera des points de mesure pourvus de sondes.

Nous devons, dans un premier temps, absolument conserver la cryptographie qui est la clef de la souveraineté, de la protection des données. La cryptographie n'a pas besoin d'être

souveraine partout mais de confiance « nationale ». Reste que c'est elle qui sécurisera les transactions et protégera les données de nos entreprises, et de nos citoyens. Idem en matière d'objets connectés, c'est un élément fondamental.

Ensuite, je l'ai dit, il s'agit pour les défenseurs d'installer des points de mesure qui nous appartiennent et qui soient validés par l'ANSSI.

Ces enjeux sont en effet particulièrement importants : ils impliquent la création de sociétés de service nationales ou alors en coopération avec des partenaires européens de confiance, ce qui reste toujours un peu délicat dans le monde des affaires mais ces sujets sont du ressort de l'ANSSI.

Mme la présidente Patricia Adam. Nous vous remercions, amiral, d'avoir répondu à l'ensemble des questions.

*

* *

La séance est levée à dix-huit heures quinze.

*

* *

Membres présents ou excusés

Présents. - Mme Patricia Adam, M. Daniel Boisserie, Mme Isabelle Bruneau, M. Jean-Jacques Candelier, M. Guy Chambefort, M. David Comet, Mme Geneviève Gosselin-Fleury, M. Christophe Guilloteau, M. Gilbert Le Bris, M. Philippe Nauche, M. Gwendal Rouillard, M. Alain Rousset, M. Jean-Michel Villaumé

Excusés. - Mme Danielle Auroi, M. Claude Bartolone, M. Philippe Briand, Mme Dominique Chauvel, M. Jean-David Ciot, M. Bernard Deflesselles, M. Guy Delcourt, Mme Carole Delga, M. Nicolas Dhuicq, Mme Geneviève Fioraso, M. Serge Grouard, Mme Edith Gueugneau, M. Francis Hillmeyer, M. Éric Jalton, M. Jean-Yves Le Déaut, M. Frédéric Lefebvre, M. Bruno Le Roux, M. Maurice Leroy, Mme Lucette Lousteau, M. Alain Marty, M. Damien Meslot, Mme Marie Récalde, M. François de Rugy, M. Philippe Vitel