N° 158

SÉNAT

SESSION ORDINAIRE DE 2013-2014

Enregistré à la Présidence du Sénat le 21 novembre 2013

AVIS

PRÉSENTÉ

au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur le projet de **loi de finances** *pour* **2014**, *ADOPTÉ PAR L'ASSEMBLÉE NATIONALE,*

TOME XII

COORDINATION DU TRAVAIL GOUVERNEMENTAL

Par MM. Jacques BERTHOU et Jean-Marie BOCKEL,

Sénateurs.

(1) Cette commission est composée de : M. Jean-Louis Carrère, *président ;* MM. Christian Cambon, Jean-Pierre Chevènement, Robert del Picchia, Mme Josette Durrieu, MM. Jacques Gautier, Robert Hue, Jean-Claude Peyronnet, Xavier Pintat, Yves Pozzo di Borgo, Daniel Reiner, *vice-présidents ;* Mmes Leila Aïchi, Joëlle Garriaud-Maylam, MM. Gilbert Roger, André Trillard, *secrétaires ;* M. Pierre André, Mme Kalliopi Ango Ela, MM. Bertrand Auban, Jean-Michel Baylet, René Beaumont, Pierre Bernard-Reymond, Jacques Berthou, Jean Besson, Michel Billout, Jean-Marie Bockel, Michel Boutant, Jean-Pierre Cantegrit, Luc Carvounas, Pierre Charon, Marcel-Pierre Cléach, Raymond Couderc, Jean-Pierre Demerliat, Mme Michelle Demessine, MM. André Dulait, Hubert Falco, Jean-Paul Fournier, Pierre Frogier, Jacques Gillot, Mme Nathalie Goulet, MM. Alain Gournac, Jean-Noël Guérini, Joël Guerriau, Gérard Larcher, Robert Laufoaulu, Jeanny Lorgeoux, Rachel Mazuir, Christian Namy, Alain Néri, Jean-Marc Pastor, Philippe Paul, Bernard Piras, Christian Poncelet, Roland Povinelli, Jean-Pierre Raffarin, Jean-Claude Requier, Richard Tuheiava, André Vallini.

Voir les numéros :

Assemblée nationale (**14**ème législ.) : **1395**, **1428** à **1435** et T.A. **239**

Sénat : **155** et **156** (annexe n° **9**) (2013-2014)

SOMMAIRE

Pages

Mesdames, Messieurs,

C'est la première fois que la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat présente un avis budgétaire consacré au programme 129 « coordination du travail gouvernemental » de la mission « Direction de l'action du Gouvernement », qui relève du Premier ministre.

Jusqu'à présent, cette mission ne faisait l'objet que d'un rapport au fond fait au nom de la Commission des Finances et d'un rapport pour avis, présenté au nom de la Commission des Lois.

Il est vrai que cette mission regroupe des entités très différentes dont le seul point commun est d'être rattachées au Premier ministre dans un ensemble budgétaire commun.

Pourtant, ce programme concerne de près les questions de défense et de sécurité.

Ainsi, au sein du programme 129 « coordination du travail gouvernemental », l'action 2 « coordination de la sécurité et de la défense » représente, avec 243,1 millions d'euros en autorisations d'engagement et 245,1 millions d'euros de crédits de paiement en 2014, près de la moitié des crédits du programme (533,8 millions d'euros en AE et 542 millions d'euros en CP).

Cette action 2 regroupe notamment :

- les crédits du Secrétariat général de la défense et de la sécurité nationale (SGDSN) et de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ;

- les subventions pour charges de service public de deux instituts placés sous la tutelle du SGDSN : l'Institut des Hautes études de défense nationale (IHEDN) et l'Institut national des Hautes études de la sécurité et de la justice (INHESJ) ;

- la dotation en fonds spéciaux destinés aux services de renseignement et au Groupement interministériel de contrôle (GIC), organisme dépendant du Premier ministre chargé des interceptions de sécurité.

C'est la raison pour laquelle, votre commission a décidé de se saisir pour avis de ce programme.

L'importance des questions de sécurité et de défense au sein du programme 129 mérite, en effet, un éclairage et un avis particulier de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat.

Cela devrait permettre notamment à votre commission de se pencher plus attentivement sur le rôle et les moyens du secrétariat général de la défense et de la sécurité nationale (SGDSN), qui relève du Premier ministre et qui est chargé de coordonner la préparation et de veiller à la mise en œuvre des mesures concourant à la stratégie de défense et de sécurité nationale, en liaison étroite avec la Présidence de la République.

En effet, les activités du SGDSN comprennent des aspects qui concernent directement la défense et la sécurité, tels que la lutte contre la prolifération, le contrôle des exportations de matériels de guerre et des transferts de technologies sensibles, la planification en matière de défense et de sécurité, l'entraînement et la préparation à la gestion des crises graves, la protection du secret de la défense nationale, la sécurité des communications gouvernementales, la sécurité des systèmes d'information et cyberdéfense ou encore la participation à l'élaboration de textes de doctrine et de textes normatifs en matière de défense et de sécurité nationale, etc.

Cela devrait permettre également, dans le prolongement des travaux de la commission sur la cyberdéfense, de suivre attentivement l'évolution des moyens consacrés à la cyberdéfense, au travers des dotations et des effectifs de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Il ne faut pas négliger non plus l'intérêt de ce programme concernant le suivi des moyens des services de renseignement, notamment à travers les fonds spéciaux destinés aux services de renseignement.

I. LE SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN) ET L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

A. LE SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN)

Le Secrétaire général de la défense et de la sécurité nationale (SGDSN)[1], dont le rôle a été confirmé par le nouveau Livre blanc sur la défense et la sécurité nationale, a pour mission d'assister le Chef du Gouvernement, en liaison étroite avec la Présidence de la République, dans les domaines de la défense et de la sécurité nationale. Ses attributions principales sont fixées par le code de la défense et recouvrent deux fonctions essentielles :

- le secrétariat ou la participation à des instances de haut niveau en matière de défense et de sécurité présidées par le Président de la République ou par le Premier ministre ;

- la prise en charge de responsabilités transverses d'animation ou d'expertise du niveau du Premier ministre en matière de défense et de sécurité.

À ce titre, il assure le secrétariat des conseils de défense et de sécurité dans leurs formations plénière, restreinte ou spécialisée. En outre, il préside les instances chargées d'étudier les questions relatives aux exportations d'armement, appuie l'action du coordonnateur national du renseignement et assure la protection du secret de la défense nationale.

L'actuel SGDSN est M. Francis Delon, qui a été entendu lors d'une audition par votre commission[2].

Le SGDSN préside plusieurs commissions techniques et organise, sous l'autorité du cabinet du Premier ministre, un nombre important de réunions interministérielles dont il assure le secrétariat, l'animation ou la présidence. Il participe à l'élaboration de textes européens[3], législatifs ou réglementaires. La conception de nombreux projets de décrets, de circulaires ou d'instructions[4] intéressant la défense et la sécurité nationale est faite ou coordonnée par le SGDSN.

---

[1] *Décret n° 2009-1657 du 24 décembre 2009 relatif au conseil de défense et de sécurité nationale et au secrétariat général de la défense et de la sécurité nationale.*

[2] *Le compte rendu de l'audition de M. Francis Delon figure en annexe au présent rapport*

[3] *Entre janvier 2012 et juillet 2013, le SGDSN a été un acteur clé dans l'élaboration des normes européennes sur la commercialisation et l'utilisation de précurseurs d'explosifs et du projet de directive, en cours d'examen, relative à l'utilisation des données des dossiers passagers (dites « données PNR »).*

[4] *Exemples de projets de circulaires et instructions : IGI 2102 (protection en France des informations classifiées de l'UE), IGI 1300 (protection en France du secret de la défense nationale),*

Les différentes directions du SGDSN (Protection et sécurité de l'Etat, Affaires internationales et stratégiques) furent en 2012 et 2013 particulièrement impliquées dans les travaux d'élaboration du nouveau Livre blanc sur la défense et la sécurité nationale. En amont des travaux de la commission du Livre blanc, le SGDSN a piloté les travaux interministériels d'actualisation du contexte stratégique, publiés en février 2012.

Outre la participation du Secrétaire général aux travaux en qualité de membre de la Commission chargée d'élaborer le Livre blanc, le secrétariat général a été impliqué dans les sept groupes de travail mis en place par la Commission chargée d'élaborer le nouveau Livre blanc. À l'issue de la remise du document au Président de la République, le SGDSN a ensuite animé le processus de validation interministérielle du nouveau Livre blanc.

Dans le prolongement de ces travaux, le SGDSN est désormais chargé de la mise en œuvre des recommandations portant sur ses attributions dans le domaine de la sécurité nationale (contrat général interministériel, démarche capacitaire territoriale, établissement d'une filière industrielle de technologies de sécurité), de l'anticipation des crises de toutes natures et du pilotage de la prospective interministérielle ou encore de la sécurité des systèmes d'information.

Les travaux de coordination interministérielle sous l'autorité du cabinet du Premier ministre se sont poursuivis pour décliner les orientations du Livre blanc dans le projet de loi relatif à la programmation militaire (LPM) pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale, qui a été adopté en première lecture par le Sénat dans la nuit du 21 au 22 octobre dernier.

1. Le SGDSN : un outil du Gouvernement pour le traitement des sujets sensibles en matière de défense et de sécurité nationale

a) Le SGDSN assure le secrétariat des Conseils de défense et de sécurité dans leurs différents formats

Le SGDSN assure le secrétariat des conseils de défense et de sécurité dans leurs formations plénière, restreinte ou spécialisée.

Cette instance, présidée par le Président de la République, est compétente pour toutes les questions de défense et de sécurité, qu'il s'agisse de la programmation militaire, de la politique de dissuasion, de la programmation de sécurité intérieure, de la sécurité économique et énergétique, de la lutte contre le terrorisme ou de la planification de réponse aux crises.

IGI 2100 (protection en France des informations classifiées de l'OTAN), IGI 6600 (sécurité des activités d'importance vitale).

Au cours des douze derniers mois, elle a notamment préparé les travaux permettant de valider le Livre blanc de la défense et de la sécurité nationale. Pendant cette même période, le Conseil de défense a été au cœur de la préparation du projet de loi de programmation militaire.

En lien plus direct avec l'actualité internationale et opérationnelle, le Conseil, dans sa formation restreinte, a eu l'occasion de se réunir pour examiner les orientations à prendre pour la conduite des crises diverses, comme celles du Mali, de la Syrie ou de la République centrafricaine.

Le Conseil de défense et de sécurité nationale comporte deux formations spécialisées qui traitent de sujets spécifiques avec une composition adaptée : d'une part, le Conseil des armements nucléaires, qui traite des questions de dissuasion et, d'autre part, le Conseil national du renseignement, qui a tenu sa première réunion en juin dernier.

b) Le SGDSN assure le suivi des crises internationales

Le SGDSN dispose d'une capacité d'analyse et de synthèse, de veille, d'alerte et d'appui à la décision relatives aux questions de sécurité internationale. Ses travaux sont principalement menés en réponse à des mandats confiés par le cabinet du Premier ministre ou par la présidence de la République.

La direction « Affaires internationales et stratégiques » du SGDSN suit les conflits et les crises internationales susceptibles d'affecter les intérêts français, en particulier ceux dans lesquels nos forces sont engagées. Elle anime des groupes interministériels d'analyse sur les crises affectant le monde arabe, l'Iran ainsi que sur les zones sahélo-saharienne et afghano-pakistanaise.

En fonction de l'actualité, elle peut être sollicitée pour produire des synthèses sur l'évolution de la situation sur certains théâtres d'opération. C'est par exemple le cas depuis janvier 2013 avec la diffusion quotidienne, puis hebdomadaire, d'une synthèse de la situation au Sahel.

Cette direction assure la coordination interministérielle de questions d'ordre stratégique, telles que le terrorisme, la défense anti-missiles balistiques, le développement du recours aux entreprises de services de sécurité et de défense, la protection des navires dans les zones à risques. Elle est chargée sur ces dossiers de proposer au Président de la République et au Gouvernement des orientations et arbitrages.

c) Le SGDSN participe à la lutte contre la prolifération et au contrôle des exportations de matériels de guerre

Le SGDSN assure aussi une veille scientifique et technique permanente dans les domaines nucléaire, radiologique, biologique et chimique, des explosifs (NRBCE), des missiles et spatial. Il coordonne ou concourt activement aux actions interministérielles portant sur la lutte contre

la prolifération, la protection du potentiel scientifique et technique de la nation, la sécurité du programme européen de navigation par satellite GALILEO et le contrôle des exportations de biens et technologies à double usage, ainsi que des images spatiales.

Le SGDSN a poursuivi ses travaux en matière de lutte contre la prolifération des armes de destruction massive et de leurs vecteurs en coordonnant les études sur ce sujet, et en produisant des documents de synthèse sur les dossiers d'actualité, notamment ceux portant sur l'Iran, la Syrie et la Corée du nord.

Dans le domaine chimique, le SGDSN assure le secrétariat du comité interministériel pour l'application de la convention sur l'interdiction des armes chimiques (CIAC). Dans le domaine biologique, le SGDSN coordonne les travaux portant sur la biologie de synthèse.

Le SGDSN assure la coordination de la réponse nationale à l'initiative internationale PSI (*Proliferation Security Initiative*). La PSI consiste à échanger entre pays membres des informations sur des transits par voie maritime de cargaisons proliférantes et à faciliter leur interception. La fréquence de ces interceptions ne cesse de croitre depuis la mise en œuvre de la PSI. Huit affaires d'interception de biens proliférants ont été menées dans ce cadre depuis l'été 2012.

La France dispose d'une importante base industrielle et technologique de défense qui contribue à la préservation de notre souveraineté, participe à la croissance économique et représente des dizaines de milliers d'emplois. Le soutien aux exportations est une nécessité mais ne saurait intervenir sans un contrôle garantissant le principe de responsabilité et le respect de nos engagements internationaux. C'est pourquoi, l'exportation de matériels de guerre est soumise à une procédure d'autorisation préalable par décision du Premier ministre (ou, par délégation, du Secrétaire général de la défense et de la sécurité nationale) après avis de la commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG). Le SGDSN assure le secrétariat de la CIEEMG et coordonne les réflexions sur la mise à jour des orientations de notre politique d'exportation.

Les travaux de modernisation du dispositif de contrôle des exportations de matériels de guerre découlant de la loi du 22 juin 2011 se poursuivent. En 2014, un système simplifié de licence unique d'exportation et de transferts intracommunautaires remplacera le mécanisme actuel.

Par ailleurs et conformément aux conclusions du Livre blanc de 2013, le SGDSN contribue à une réflexion plus générale sur le renforcement du contrôle des exportations de biens et technologies à double usage et participe à la totalité des commissions interministérielles des biens à double usage (CIBDU). La France a obtenu, dans le cadre de l'Arrangement de WASSENAAR, que les outils de surveillance et de contrôle de l'internet

soient soumis à autorisation avant leur exportation. Le SGDSN avait déjà favorisé en 2011 l'inscription dans la liste des biens soumis à contrôle des matériels d'interception des communications téléphoniques mobiles.

2. Le SGDSN contribue à la politique de sécurité nationale

a) La rénovation des plans de protection de la « famille pirate » dont le plan VIGIPIRATE de lutte contre le terrorisme

Dans la continuité du travail engagé en 2012 pour rénover les plans gouvernementaux, le SGDSN a notamment initié une révision en profondeur du plan VIGIPIRATE sur mandat du Premier ministre. Cette révision doit aboutir fin 2013 à un nouveau plan VIGIPIRATE qui gardera les principes qui font la force du plan actuel mais qui sera rendu plus efficace par une meilleure visibilité. Il s'agit de rendre publique une grande partie du plan et de renforcer la communication sur la menace terroriste et sur les mesures prises. Le pilotage des postures de protection sera également amélioré par une caractérisation plus fine des menaces terroristes et des vulnérabilités. Dans les deux ans à venir, ce nouveau plan VIGIPIRATE sera complété par la révision progressive des plans d'intervention de la famille «PIRATE» (Pirate-air, Pirate-mer, Piranet,…), à l'exception du plan NRBC qui date de 2011.

Ce travail de planification est notamment complété, en matière de lutte contre le terrorisme, par un effort spécifique dans le domaine de la sûreté du transport aérien et une relance des travaux interministériels relatifs à la protection contre les menaces NRBC-E.

b) Mandat radicalisation

Le Premier ministre a confiée au SGDSN, en août dernier, une mission relative à la mise en œuvre d'une stratégie nationale de prévention de la radicalisation. Il s'agit notamment de formuler des propositions visant à développer une politique d'identification et de réduction des vulnérabilités des individus et des groupes face aux idées radicales de toute nature pouvant déboucher sur l'action violente.

Lancés début septembre, les travaux associent l'ensemble des ministères concernés et permettent une analyse des dispositifs existants en les comparant avec les initiatives étrangères. Ces analyses et propositions nourriront la réflexion du Gouvernement en vue d'élaborer une stratégie nationale de prévention de la radicalisation.

c) L'amélioration de l'organisation gouvernementale de réponse aux crises majeures

Le Livre blanc de 2013 a réaffirmé la pertinence du concept de sécurité nationale. Dans ce cadre, l'organisation gouvernementale de gestion de crise a été consolidée. Un effort de professionnalisation des acteurs de la gestion de crise est engagé depuis 2012. Cette démarche se fonde à la fois sur

des exercices majeurs rénovés et sur des entraînements spécifiques permettant de former les personnels armant la cellule interministérielle de crise (CIC).

Les premiers effets positifs de ce programme global de professionnalisation ont pu être mesurés lors des derniers exercices majeurs, ainsi qu'au travers du bon fonctionnement de la CIC lors des dernières crises, à l'exemple de l'épisode neigeux de l'hiver 2012-2013.

L'amélioration de la connaissance des menaces et des risques, de la veille et de l'anticipation constitue également un enjeu spécifique dans la préparation et la réponse de l'Etat aux crises. Dans ce domaine, le SGDSN a poursuivi son action de développement d'une culture d'anticipation des crises au sein des ministères.

d) Le développement de la résilience et le renforcement de la continuité des activités essentielles à la Nation

La gestion de crise s'accompagne d'un renforcement de la résilience qui doit être perçu à la fois comme un objectif (renforcer la cohésion et la solidité de la Nation face aux risques et menaces) et comme une méthode (mobiliser tous les acteurs).

Pour atteindre ce double objectif, le SGDSN a initié en 2012 les travaux visant à instaurer une politique nationale de résilience associant tous les acteurs. Cette politique s'appuie sur le dispositif de sécurité des activités d'importance vitale (SAIV), ainsi que sur des actions complémentaires permettant d'améliorer la continuité des activités indispensables à la Nation.

Au terme d'une très large consultation des acteurs publics et privés, le SGDSN a publié un guide d'aide à l'élaboration des plans de continuité d'activité (PCA) à destination des administrations, des collectivités et des entreprises.

e) L'élaboration d'un contrat général interministériel (CGI)

Les travaux de la commission du Livre blanc ont fixé une feuille de route qui se traduit par le lancement de nouveaux chantiers interministériels dont le contrat général interministériel qui déterminera, dans une perspective de programmation budgétaire, les capacités « critiques » des ministères civils et leur niveau d'engagement dans la réponse aux crises majeures. Il s'appliquera aux capacités des ministères civils détenues au niveau national.

La démarche conduite dans le cadre du CGI sera prolongée à l'horizon 2016 sous l'autorité du ministre de l'intérieur par une planification territoriale de gestion des crises. Cette démarche capacitaire permettra d'associer plus étroitement qu'aujourd'hui l'ensemble des acteurs à la préparation et à la gestion des crises et assurera une meilleure cohérence entre la planification gouvernementale et la planification locale.

f) La filière industrielle de sécurité

Dans la continuité de son rôle de pilotage des positions françaises au sein du programme européen de recherche en sécurité, le SGDSN prend une part active dans la structuration de la filière industrielle de sécurité française. Il a ainsi préparé la mise en place du comité de la filière industrielle de sécurité (COFIS), installé en octobre dernier par le Premier ministre.

Rassemblant autour du Premier ministre, onze ministres, vingt et un présidents directeurs généraux de sociétés développeuses ou utilisatrices de solutions de sécurité, cinq présidents de groupements industriels et dix-neuf personnalités qualifiées, dont des représentants de la recherche académique, la présidente de la commission informatique et liberté et plusieurs parlementaires, le CoFIS mobilisera tous les secteurs technologiques et toutes les compétences publiques et privées nécessaires pour soutenir le développement de solutions de sécurité, fiables, compétitives, adaptées aux besoins des utilisateurs nationaux et respectueuses des droits et libertés fondamentaux.

B. L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

La perception de plus en plus aiguë des risques engendrés par le développement des systèmes d'information, confortée par l'explosion du nombre d'intrusions informatiques contre les infrastructures nationales, a conduit à créer en 2009, à la suite du précédent Livre blanc sur la défense et la sécurité nationale de 2008, une agence nationale de la sécurité des systèmes d'information[1] (ANSSI). Autorité nationale de défense des systèmes d'information, elle est chargée 24 heures sur 24 de prévenir et de réagir aux attaques contre nos infrastructures critiques. Elle est dirigée par M. Patrick Pailloux.

Rattachée au secrétaire général de la défense et de la sécurité nationale, son domaine d'intervention initialement centré sur les administrations et les organismes dépendant de l'État s'est rapidement élargi aux opérateurs d'importance vitale (OIV) et aux entreprises indispensables à notre stratégie de sécurité nationale. Le centre de transmission gouvernemental (CTG), mis pour emploi auprès de l'ANSSI, met en œuvre une partie des systèmes de télécommunications sécurisés nécessaires à la continuité de l'action de l'État.

[1] *Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé « Agence nationale de la sécurité des systèmes d'information ».*

1. La cyberdéfense : une priorité nationale

a) Une menace majeure

Avec le développement de l'Internet, les systèmes d'information constituent aujourd'hui de véritables « centres nerveux » de nos sociétés, sans lesquels elles ne pourraient plus fonctionner.

Or, il apparaît aujourd'hui que le développement des systèmes d'information et leur interconnexion croissante, dans toutes les formes d'activités, ont souvent été réalisés au détriment des exigences de sécurité.

Depuis les attaques informatiques massives qui ont frappé l'Estonie en avril 2007, l'actualité s'est chargée de nous montrer la réalité de cette menace.

Il ne se passe pratiquement pas une semaine sans que l'on signale, quelque part dans le monde, des attaques ciblées contre les réseaux de gouvernements ou de grands organismes publics ou privés.

Depuis la publication du rapport d'information sur la cyberdéfense, présenté par votre commission en juillet 2012[1], le thème de la cybersécurité n'a d'ailleurs pas cessé de prendre de l'ampleur.

On peut distinguer quatre types d'attaques informatiques :

- tout d'abord, tout ce qui relève de la cybercriminalité, qui regroupe par exemple la fraude bancaire ou la pédopornographie sur Internet, et qui est en plein essor. Selon la Commission européenne, la cybercriminalité ferait plus d'un million de victimes chaque jour dans le monde ;

- deuxième objectif de l'attaquant : la déstabilisation. C'est l'attaque la plus souvent médiatisée car la plus visible : des messages de propagande ou d'hostilité sont placés sur des sites internet mal protégés à l'occasion de telle décision politique ou d'un conflit armé. C'est notamment le cas des attaques menées par le groupe *Anonymous* ;

- troisième objectif visé par les attaquants : le sabotage. L'attaquant cherche alors à faire dysfonctionner les installations connectées aux réseaux de communications électroniques. Certaines de ces cyberattaques peuvent mettre en cause la sécurité nationale : les attaques sur des systèmes étatiques, sur des réseaux essentiels touchant à des infrastructures critiques (comme une centrale électrique ou le réseau d'électricité par exemple), voire des systèmes de communication de nos équipements militaires ; depuis 2010, nous connaissions le programme STUXNET qui aurait détruit un millier de centrifugeuses de la centrale nucléaire iranienne de Natanz. Mais, en août dernier, deux attaques informatiques d'ampleur ont visé des sociétés du

[1] *Rapport d'information n°681 (2011-2012) sur la cyberdéfense présenté par M. Jean-Marie Bockel au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, le 18 juillet 2012.*

secteur de l'énergie au Moyen-Orient, dont le premier producteur mondial de pétrole Saudi Aramco. 30 000 ordinateurs ont été rendus inutilisables en quelques heures ;

- enfin, dernier type d'attaque, le cyberespionnage. Cet espionnage, souvent d'origine étatique, est massif, comme l'illustrent les révélations de l'ex-consultant de la NSA, Edward Snowden, sur le vaste programme d'espionnage informatique américain PRISM. En matière industrielle, il atteint tous nos secteurs de souveraineté.

La France n'est pas épargnée par ce phénomène.

On estime que nos administrations, nos entreprises ou nos opérateurs d'importance vitale sont victimes chaque jour de plusieurs millions d'attaques informatiques. Certaines de ces attaques prennent la forme d'une prise de contrôle durable et d'une exfiltration massive de données sensibles

D'une manière générale, les attaques informatiques peuvent être menées par des pirates informatiques, des groupes d'activistes, des organisations criminelles, mais aussi par des entreprises concurrentes, voire par d'autres Etats.

Cette cybermenace ira inévitablement en s'accentuant, pour plusieurs raisons :

- nous sommes tous les jours plus dépendants des systèmes d'information et d'internet, ce qui en fait des cibles particulièrement sensibles ;

- l'interconnexion des réseaux est croissante et l'utilisation de produits standards, dont les vulnérabilités sont en permanence scrutées par les attaquants, se généralise ;

- le profil des attaquant se professionnalise, avec l'apparition de véritables groupes de hackers capables de monnayer leur savoir-faire auprès d'un large éventail de commanditaires ;

- certains Etats eux-mêmes se dotent de capacités offensives ;

- enfin, ce type d'attaque reste peu coûteux et peu risqué pour celui qui le met en œuvre.

Pour ces raisons, votre commission recommandait dans son rapport d'information, à l'été 2012, de faire de la cyberdéfense une véritable priorité nationale et proposait 50 recommandations concrètes et 10 priorités.

b) Le nouveau Livre blanc

Le nouveau Livre blanc sur la défense et la sécurité nationale, publié en avril 2013, marque une nouvelle étape dans la prise en compte par les pouvoirs publics des questions liées à la cybersécurité.

Dans sa préface, le Président de la République y affirme la nécessité de protéger les Français *« y compris face aux risques de la cybermenace »* présentée dans l'introduction comme pouvant *« affecter gravement la sécurité de la Nation ».*

Parmi les priorités identifiées par le nouveau Livre blanc figurent notamment :

- le renforcement des moyens humains qui sont consacrés à la défense et à la sécurité de nos systèmes d'information, *« à la hauteur des efforts consentis par nos partenaires britannique et allemand »* ;

- *« la capacité de produire en toute autonomie nos dispositifs de sécurité, notamment en matière de cryptologie et de détection d'attaque »* ;

- une politique des systèmes d'information de l'Etat qui *« s'appuiera notamment sur le maintien de réseaux de haute sécurité irrigant les autorités de l'État, sur une politique appropriée d'achat public et sur une gestion adaptée des équipements de communications mobiles »* ;

- pour renforcer le niveau de sécurité des systèmes d'information des infrastructures critiques nationales, *« l'État fixera, par un dispositif législatif et réglementaire approprié, les standards de sécurité à respecter à l'égard de la menace informatique et veillera à ce que les opérateurs prennent les mesures nécessaires pour détecter et traiter tout incident informatique touchant leurs systèmes sensibles. »*. Les opérateurs concernés devront notifier ces incidents et l'agence nationale de la sécurité des systèmes d'information (ANSSI) ou d'autres services de l'Etat pourront intervenir en cas de crise grave ;

- un approfondissement de nos relations avec nos partenaires privilégiés et, au niveau européen, le soutien à la mise en place d'une politique européenne de cybersécurité.

Enfin, le Livre blanc précise qu' *« une attention particulière sera portée à la sécurité des réseaux de communication électroniques et aux équipements qui les composent ».*

c) Une priorité européenne

La Commission européenne a présenté le 7 février 2013 une stratégie européenne de cybersécurité et une proposition de directive européenne en matière de sécurité des réseaux et des systèmes d'information (COM (2013) 48 final).

Dans son chapitre IV, cette proposition de directive prévoit l'extension à un ensemble d'« opérateurs de marché » des dispositions

prévues par les articles 13 a et b de la directive cadre du paquet Télécom, en particulier :

- l'instauration du principe de notification obligatoire d'incidents informatiques significatifs par les opérateurs économiques visés par la directive ;

- l'introduction de la possibilité pour l'autorité nationale de cybersécurité ou pour des prestataires qualifiés de conduire des audits réguliers et d'exiger la mise à disposition par les opérateurs des informations nécessaires à la conduite des audits ;

- l'introduction du principe de « sanction » en cas de non-respect de ces dispositions.

Ces orientations ont été approuvées par votre commission dans un rapport présenté par vos deux rapporteurs pour avis[1] et ont donné lieu à une résolution du Sénat du 19 avril 2013.

d) Les dispositions de la Loi de programmation militaire

Dans le prolongement du nouveau Livre blanc sur la défense et la sécurité nationale, le chapitre III du projet de loi relatif à la programmation militaire pour les années 2014 à 2019 contient des *« Dispositions relatives à la protection des infrastructures vitales contre la cybermenace ».*

Quatre principales dispositions sont proposées.

Tout d'abord, les dispositions prévues visent à préciser les responsabilités du Premier ministre en matière de défense et de sécurité des systèmes d'information.

Elles visent également, en cas d'attaque informatique grave, à donner aux agents appartenant aux services de l'Etat compétents en matière de sécurité et de défense des systèmes d'information, désignés par le Premier ministre, la capacité à mener les opérations techniques nécessaires à la caractérisation de cette attaque ou à la limitation de ses effets. Dans une situation où l'attaquant a généralement l'avantage sur le défenseur, les agents de l'Etat en charge de la sécurité et de la défense des systèmes d'information doivent pouvoir être en mesure d'utiliser toutes leurs capacités pour mieux appréhender la nature et l'ampleur d'une attaque et la motivation de son ou de ses auteurs et d'en prévenir, d'en atténuer les effets ou de la faire cesser lorsque les circonstances l'exigent.

Le projet de LPM a également pour objectif d'amener les opérateurs d'importance vitale à respecter des règles de sécurité informatique, conjointement élaborées par l'ANSSI avec les opérateurs concernés sous le pilotage du ministère coordonnateur du secteur, nécessaires à la protection

[1] *Rapport n°491 (2012-2013) de MM. Jacques Berthou et Jean-Marie Bockel, fait au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, déposé le 10 avril 2013 et proposition de résolution européenne n°138 (2012-2013).*

des systèmes d'information essentiels à leur cœur de métier. Ces règles pourront comprendre la mise en œuvre d'un système de détection d'attaques informatiques.

Le projet impose aux opérateurs d'importance vitale la notification des incidents informatiques qui touchent leurs systèmes d'information critiques. Cette notification permettra d'identifier les attaques informatiques nécessitant une intervention de l'ANSSI, d'une autre administration de l'État ou d'un prestataire.

Le texte d'application précisera par secteur d'activité le type d'incidents à notifier, les niveaux de gravité et les délais dans lesquels ces incidents devront être déclarés. La confidentialité des informations fournies par les opérateurs sera préservée.

Le texte du projet de loi donne la capacité aux acteurs désignés d'effectuer les audits permettant, notamment, d'évaluer le niveau de sécurité des systèmes d'information visés par les articles précédents, voire de détecter l'éventuelle compromission de ces systèmes, et de vérifier que les règles édictées sont bien respectées.

Le projet de LPM donne au Premier ministre la capacité d'imposer, en cas de crise majeure concernant les systèmes d'information, des mesures techniques que les opérateurs d'importance vitale seront tenus de mettre en œuvre. En effet, dans les crises auxquelles l'État se prépare, les attaques informatiques ont une cinétique et une capacité d'expansion particulière. Des exemples d'attaques récentes montrent que, en quelques minutes, des dizaines de milliers d'ordinateurs d'un opérateur peuvent être mis hors d'état de fonctionnement tandis qu'un programme informatique malveillant peut se diffuser dans des systèmes d'information du monde entier en quelques heures.

Le texte prévoit des sanctions visant les personnes physiques et morales manquant aux obligations prévues.

Enfin, il est proposé d'étendre le contrôle étatique aux équipements informatiques permettant de réaliser des interceptions, même si cette capacité n'est pas leur fonction essentielle.

Ces dispositions ont été approuvées par votre commission des affaires étrangères, de la défense et des forces armées, puis par le Sénat, lors de l'adoption du projet de loi de programmation militaire.

A l'initiative de la commission des affaires étrangères, de la défense et des forces armées du Sénat, les dispositions du projet de LPM relatives à la cybersécurité ont été complétées sur deux aspects :

- en permettant à l'ANSSI d'accéder aux coordonnées des utilisateurs d'adresses internet à des fins de prévention ou de traitement des attaques informatiques ;

- en clarifiant le régime juridique en matière d'activités économiques ou de recherche portant sur la sécurité des systèmes informatiques.

Parallèlement, votre commission a souhaité préciser, dans le rapport annexé, l'augmentation des moyens humains consacrés à la cyberdéfense, tant de l'ANSSI qu'au sein des armées.

2. Les missions de l'ANSSI

Les missions de l'ANSSI sont fixées dans le décret n° 2009-834 du 7 juillet 2009 portant création de cette agence, modifié par le décret n° 2011-170 du 11 février 2011.

L'ANSSI, autorité nationale en matière de sécurité et de défense des systèmes d'information, a la responsabilité de conduire ou de coordonner l'ensemble des actions destinées à prévenir la réussite des attaques contre les systèmes d'information, et à réagir en cas d'atteinte à leur disponibilité ou à leur intégrité. Son action s'exerce principalement au profit de l'État, mais vise également les opérateurs d'importance vitale du secteur privé et, plus généralement, l'ensemble des acteurs de la société de l'information.

a) En amont

Dans le domaine de la prévention des attaques informatiques, l'ANSSI est principalement chargée :

• d'élaborer les règles et les mesures à appliquer pour la protection des systèmes d'information de l'État, et d'en vérifier l'application ;

• de développer et d'acquérir les produits essentiels à la protection des systèmes d'information les plus sensibles de l'État (autres que ceux spécifiquement militaires) ;

• de concevoir, de faire réaliser et de mettre en œuvre les moyens interministériels sécurisés de communications électroniques nécessaires au Président de la République et au Gouvernement, notamment le réseau téléphonique Rimbaud et l'intranet ISIS. Elle dispose à cette fin pour emploi du centre de transmissions gouvernemental (CTG) ;

• d'assister les administrations et les opérateurs d'importance vitale (OIV) dans la sécurisation de leurs systèmes d'information ;

• de mener des audits et des inspections des systèmes d'information ;

• de délivrer des labels aux produits et aux mécanismes de sécurité destinés à protéger les informations, notamment celles couvertes par le secret de la défense nationale, et les systèmes qui les traitent, ainsi qu'aux prestataires de services de confiance qui interviennent dans les domaines des technologies de l'information. Elle établit dans ce but des référentiels

techniques dans tous les domaines de la sécurité des systèmes d'information ;

• de contribuer à la sensibilisation des agents de l'État et d'assurer la formation de ses experts dans les divers aspects de la sécurité des systèmes d'information ;

• de contribuer au développement de la confiance dans l'économie numérique ;

• de contribuer à la promotion des technologies, des systèmes et des savoir-faire nationaux ;

• de promouvoir, en liaison avec les ministères concernés, la cybersécurité dans l'enseignement supérieur et dans la recherche.

b) En aval

Dans le domaine de la réaction aux attaques informatiques, l'ANSSI est principalement chargée d'exercer la fonction d'autorité nationale de défense des systèmes d'information et, à ce titre, de décider des mesures que l'État met en œuvre pour répondre aux crises affectant ou menaçant la sécurité des systèmes d'information des autorités publiques et des opérateurs d'importance vitale et de coordonner l'action gouvernementale en cas d'attaque ou de compromission des systèmes. L'agence s'appuie sur :

• un système de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de l'État et des opérateurs d'importance vitale ;

• un réseau d'alerte permanent permettant l'échange rapide d'informations techniques et opérationnelles utiles à la cybersécurité ;

• des groupes d'intervention rapide en mesure de rechercher et de détecter les compromissions affectant les systèmes d'information de l'État et des opérateurs d'importance vitale, de superviser les opérations de traitement d'incident ou de reconstruction des systèmes compromis, et éventuellement de porter assistance à nos alliés en cas de crise informatique.

3. Les principales actions réalisées ou engagées en 2012 et 2013

a) La réponse aux attaques

Le centre de détection des attaques informatiques, entré en phase opérationnelle début 2010, a augmenté sa couverture en équipant les réseaux de nouveaux ministères et a amélioré ses capacités techniques de détection.

L'ANSSI accompagne également le projet de réseau interministériel de l'Etat (RIE) sur le volet de la sécurité et a développé des sondes adaptées pour détecter les attaques qui le viseraient.

L'ANSSI a traité de très nombreuses cyberattaques majeures visant des administrations ou de grandes entreprises nationales, notamment à des fins d'espionnage, dans lesquelles les attaquants ont eu un contrôle total du système d'information.

Ces opérations, lourdes, ont pour premier objectif de reprendre le contrôle des systèmes touchés. Elles incluent non seulement une remise en état des éléments compromis, mais également un renforcement global de ce système pour éviter ou au moins retarder une reprise de contrôle ultérieure par l'attaquant.

En 2012, 27 affaires ont ainsi été traitées par l'ANSSI. **Les effectifs actuels de l'agence n'ont pas permis de traiter toutes les attaques dont elle a eu connaissance.**

L'ANSSI héberge, au sein de son centre opérationnel, le centre d'alerte et de réaction aux attaques informatiques (CERT).

Le CERT analyse les vulnérabilités (failles de sécurité) et les codes malveillants qui les exploitent. En 2012, le CERT a émis 766 avis, 10 alertes et 52 bulletins d'actualité.

Le CERT est alerté sur des incidents qui peuvent être le fait d'attaques de plus ou moins grande ampleur. Le CERT analyse des codes malveillants, effectue des synthèses des incidents traités, en tire les enseignements et propose, le cas échéant, des mesures générales de prévention. Le CERT intervient également régulièrement en matière judiciaire comme auxiliaire de justice. En 2012, le CERT a reçu plus de 700 signalements et a pu traiter directement environ 70 incidents.

Le centre opérationnel de la sécurité des systèmes d'information (COSSI) de l'ANSSI et le centre d'analyse de lutte informatique défensive (CALID) du ministère de la défense sont désormais colocalisés dans les nouveaux locaux de l'ANSSI, dans l'immeuble « Tour Mercure » dans le XVe arrondissement de Paris.

Ce rapprochement géographique renforce une collaboration déjà étroite avec le ministère de la défense et facilitera l'appui que l'état-major des armées pourra fournir à l'ANSSI, et réciproquement, notamment en cas de crise majeure.

b) La sécurisation des systèmes d'information des entreprises appartenant aux secteurs d'activité d'importance vitale

Parmi les actions concrètes menées par l'ANSSI en 2013 au profit des secteurs d'activité d'importance vitale, on peut citer :

- la mise en place d'un groupe de travail regroupant des opérateurs d'importance vitale, des équipementiers et des intégrateurs, portant sur la sécurisation des systèmes de contrôle-commande des processus industriels ;

- l'élaboration, en lien avec la direction générale de la compétitivité, de l'industrie et des services (DGCIS), d'un référentiel de sécurité du système de compteurs électriques intelligents LINKY qui sera déployé par Electricité Réseau Distribution France (ERDF) ;

- le lancement de l'élaboration d'une procédure de labellisation des prestataires d'informatique en nuage (*cloud computing*) ;

- la conduite, à la demande du ministre chargé des communications électroniques, des premiers contrôles de sécurité chez les quatre principaux opérateurs de communications électroniques. L'agence a également conduit des audits d'opérateurs dans les domaines de l'énergie et du transport ;

- la poursuite, conjointement avec l'association française pour le nommage d'internet en coopération (AFNIC), des travaux de l'Observatoire de la résilience de l'Internet français.

L'adoption définitive des dispositions prévues par le projet de loi de programmation militaire permettrait à l'ANSSI :

• d'être en mesure de suivre la conception de systèmes de détection d'attaques informatiques, de labelliser des outils de surveillance et de suivre et de former les prestataires capables de participer au traitement de cyberattaques ;

• d'élaborer, en concertation étroite avec les opérateurs concernés, des référentiels de sécurité en fonction de leur secteur d'activité et de leur nature ;

• de mettre en place les dispositifs de notification d'incidents prenant en compte le secteur d'activité et son organisation.

4. Les autres actions de l'ANSSI

a) Labellisation de produits et développement d'un tissu industriel « de confiance »

La labellisation de produit et de services constitue une brique essentielle de la sécurisation des systèmes d'information. Dans la mesure où ils sont disponibles, le choix de produits et de services labellisés est obligatoire pour toutes les autorités administratives, même si ces dernières ne respectent pas toujours cette obligation.

Le succès des certifications, tant chez les utilisateurs que chez les développeurs de produits, entraîne une augmentation du nombre de projets gérés par l'ANSSI et une saturation du centre de certification qui doit augmenter rapidement ses effectifs.

L'ANSSI qualifie aussi des prestataires de confiance en matière d'audit de la sécurité des systèmes d'information.

L'agence apporte aussi son expertise technique dans le cadre des investissements d'avenir en faveur du développement de l'économie numérique, financés par l'emprunt national (4,5 milliards d'euros).

Elle est consultée par la direction générale du trésor du ministère de l'économie et des finances lorsque des demandes d'autorisation d'investissements étrangers concernent des entreprises du secteur de la sécurité des systèmes d'information.

b) Développement et mise en œuvre de produits et de réseaux de sécurité

L'ANSSI gère les systèmes de communication de haute sécurité pour les besoins de l'État, avec le soutien du centre de transmissions gouvernemental (CTG) ainsi que les systèmes d'information internes de l'ANSSI.

Pour protéger les communications les plus importantes ou les plus secrètes des autorités, l'ANSSI a largement déployé en 2012 les téléphones sécurisés Teorem sur le réseau Rimbaud, réseau résilient de plus de 4 000 abonnés, initialement destiné aux communications de crise, capable de fonctionner même lorsque les réseaux commerciaux des opérateurs ne fonctionnent plus correctement (tempêtes, inondations, …).

Environ 2 300 téléphones ont été livrés aux ministères et plus de 1 600 sont installés et en fonction sur le réseau Rimbaud. De plus, une quarantaine de Teorem sont en fonctionnement au ministère des affaires étrangères et dans les ambassades.

S'agissant de la téléphonie mobile sécurisée de niveau inférieur à Confidentiel Défense, et compte tenu des attentes très fortes des hautes autorités en matière d'ergonomie, l'ANSSI accompagne désormais les ministères dans le choix de solutions commerciales. L'ANSSI poursuit toutefois le développement d'une expertise interne dans ce domaine.

Le réseau de données interministériel ISIS, initialement déployé pour la gestion de crises, est en cours de modernisation.

c) Le centre de transmissions gouvernemental (CTG)

Le CTG compte 180 personnels des trois armées et dispose de locaux sur les sites de la forteresse du Mont-Valérien à Suresnes et de l'hôtel national des Invalides. Organisme militaire mis pour emploi auprès de l'ANSSI, le CTG intervient dans la mise à disposition d'une partie des systèmes de télécommunication sécurisés nécessaires à la continuité de l'action de l'État.

En 2012, le CTG a maintenu à très haut niveau de disponibilité les systèmes déployés au profit du chef de l'État et du chef du gouvernement lors de leurs déplacements en France ou à l'étranger. Le CTG a continué d'apporter son expertise technique dans les différents programmes auxquels il participe ou qu'il conduit pour le compte du SGDSN :

- la réalisation d'un réseau gouvernemental à haute disponibilité ;

- le suivi du projet relatif au traitement interministériel des messages de niveau secret défense ;

- la modernisation des moyens de communications présidentielles et du Premier ministre pour les différents types de déplacement.

d) Formation et sensibilisation

L'ANSSI mène une politique de communication de plus en plus active. Cette communication qui vise à sensibiliser les acteurs passe aujourd'hui par la publication de documents, des interventions dans les médias ou des conférences et la présence sur des salons. Des opérations de sensibilisation ciblées sont également conduites vers les entreprises. Enfin des opérations de communication sont spécifiquement menées à des fins de recrutement.

L'ANSSI, grâce à son centre de formation à la sécurité des systèmes d'information (CFSSI), sensibilise et forme des acteurs publics à la SSI. En 2012, le CFSSI a accueilli 1 500 stagiaires de l'administration sur une vingtaine de sujets, pour des durées allant d'une journée à cinq semaines et un objectif allant de la sensibilisation à l'acquisition d'une expertise.

Le CFSSI forme par an, au profit des administrations, 8 à 10 experts en sécurité des systèmes d'information (ESSI) par un enseignement long (13 mois). Le même titre est délivré par l'École Télécom Sud Paris dans le cadre d'un partenariat avec l'ANSSI.

Parmi les documents publiés, il convient de signaler la diffusion du « guide d'hygiène informatique ». Ce guide donne 40 mesures simples qui doivent impérativement être appliquées par toutes les organisations publiques et/ou privées qui estiment devoir un minimum protéger leurs systèmes d'information. Ce document est la référence de la communication de l'ANSSI.

C. LES EFFECTIFS ET LE BUDGET DU SGDSN ET DE L'ANSSI

1. Le budget du SGDSN et de l'ANSSI

Dans le cadre de la loi de finances de 2013, le SGDSN devait bénéficier de crédits à hauteur de 195 millions d'euros en autorisations d'engagement et de 200 millions d'euros en crédits de paiement.

La réserve de précaution, d'un montant initial de 8,5 millions d'euros en AE et de 8,8 millions d'euros en CP en début de gestion, a été abondée dès février 2013 de 7,8 millions d'euros en AE et en CP au titre d'un gel supplémentaire de crédits sur décision du Premier ministre. Le budget du SGDSN a donc été amputé de 16,55 millions d'euros en AE et en CP.

Les transferts de crédits vers le ministère de la défense se sont élevés à 56,56 millions d'euros en AE et 64,56 millions d'euros en CP.

Au total, les crédits disponibles étaient de 122 millions d'euros en AE et 118,6 millions d'euros en CP, et les prévisions de consommation au 31 décembre 2013 étaient de 105 millions d'euros en AE et 112 millions d'euros en CP.

Les perspectives budgétaires du SGDSN pour 2014 et 2015 se présentent de la manière suivante :

Montants en AE et CP (en millions d'€)

	PLF 2014		**LPFP 2015**	
	AE	CP	AE	CP
Dépenses de personnel Titre 2	47,69	47,69	45,01	45,01
Fonctionnement Titre 3	47,63	51,29	137,98	148,37
Investissements Titre 5	96,72	94,51		
Interventions Titre 6	1,05	1,65		
TOTAL	**191,08**	**193,13**	**182,99**	**193,38**

Le budget du SGDSN présenté dans le projet de loi de finances pour 2014 prévoit un plafond de crédits de **191 millions d'euros en autorisations d'engagement et 193 millions d'euros en crédits de paiement**.

Sur cette enveloppe, une soixantaine de millions d'euros devraient être transférés au ministère de la défense pour le financement de projets interministériels.

Les perspectives budgétaires pour 2015 correspondent aux arbitrages du Premier ministre fixés par la lettre plafond du 31 juillet 2012 relative aux autorisations de dépenses 2013-2015. Elles n'intègrent pas le schéma d'emploi de l'ANSSI en 2014 et 2015 qui n'avait pas été arrêté dans le cadre de ce budget triennal.

À la différence du budget du ministère de la défense, les crédits du SGDSN et de l'ANSSI ne font pas l'objet de projections pluriannuelles dans le cadre du projet de loi de programmation militaire 2014-2019. Les projections financières pluriannuelles du budget du SGDSN, notamment en application des orientations prévues par le livre blanc de 2013, seront définies dans le cadre du prochain budget triennal 2015-2017 qui sera élaboré l'année prochaine. Compte tenu de la forte évolutivité des technologies de l'information et de la communication et des menaces qu'elles peuvent générer, une projection triennale actualisée tous les 2 ans apparaît mieux adaptée aux besoins d'évolution du budget de l'ANSSI.

L'évolution des dépenses de personnel (titre 2), à hauteur de 47,6 millions d'euros, est principalement induite par l'évolution des effectifs du SGDSN, et en premier lieu ceux de l'ANSSI.

Dans le cadre des travaux sur le livre blanc 2013, le Président de la République a fixé l'objectif d'atteindre un effectif de l'ANSSI de 500 agents à l'horizon 2015.

Une telle mesure figurait parmi les principales recommandations de votre commission.

À cet effet, le schéma d'emploi retenu en 2014 pour l'ANSSI vise la création de 65 postes supplémentaires (ETP), soit une prévision de 422 agents à échéance de fin 2014. Cela représente l'embauche de 110 personnes par an, soit le tiers de son effectif.

Par ailleurs, le plafond d'emplois du SGDSN (hors ANSSI), relevant des orientations du Premier ministre pour les secteurs non prioritaires, subira une diminution de 3 emplois sur la période 2013-2015 (-1 ETP chaque année). Le SGDSN comptera donc 207 agents fin 2014.

L'évolution des autres dépenses (hors titre 2) applique la même dynamique.

Dans le cadre des travaux du budget triennal 2013-2015, les besoins de montée en puissance de l'ANSSI ont été préservés, confirmant la priorité accordée depuis 2009. Ainsi, les ressources en CP consacrées aux missions et activités de l'ANSSI (et du CTG) augmenteront par rapport à la loi de finances de 2012 de 21 % dans le cadre du PLF pour 2014.

Les plafonds de crédits au profit de l'ANSSI retenus par le Premier ministre à l'occasion du budget triennal 2013-2015 s'élevaient, à périmètre 2013, aux montants suivants :

- 2013 : 67,7 M€ en AE et 67,3 M€ en CP ;
- 2014 : 56,9 M€ en AE et 63,2 M€ en CP ;
- 2015 : 60,4 M€ en AE et 64,9 M€ en CP.

Les plafonds de crédits de l'ANSSI retenus par le Premier ministre en PLF 2014, révisés à l'occasion des travaux budgétaires de cette année en adéquation avec les besoins exprimés par l'agence, s'élèvent à **64,1 millions d'euros en autorisations d'engagement et 70,5 millions d'euros en crédits de paiement.** Les plafonds 2015 seront ajustés l'année prochaine dans le cadre des travaux sur le budget triennal 2015-2017.

Les ressources prévues permettent de financer à titre principal les projets innovants, dont les projets interministériels au titre du plan interministériel de modernisation des produits de sécurité gouvernementaux PMPS et au titre du programme de cryptographie nouvelle génération CNG, de développement et de mise en œuvre, d'une part, des moyens de communication sécurisée gouvernementale et intergouvernementale et,

d'autre part, des moyens de protection informatique des réseaux sensibles de l'État et des opérateurs d'importance vitale.

Elles permettent également, en liaison avec l'augmentation progressive des moyens techniques et humains de l'agence, de financer le schéma immobilier portant sur le développement des capacités d'accueil en bureaux et locaux techniques mis à la disposition de l'agence. En particulier, elle permet de financer l'installation de personnel et de moyens techniques, dont le centre national de crise cyberdéfense, dans l'immeuble « Tour Mercure » pris à bail en 2012. Par ailleurs, est également prévu le développement de capacités immobilières dans le cadre du plan de continuité des activités pour les besoins du SGDSN et de l'ANSSI.

Elles comprennent aussi la quote-part des dépenses indivises de fonctionnement courant de l'ensemble des services soutenus par le budget du SGDSN.

L'évolution des dépenses hors titre 2 est également marquée par l'importance des besoins de financement du programme pour les besoins en capacités techniques interministérielles (CTIM).

Les prévisions de transfert de crédit vers le ministère de la défense au titre des projets interministériels sont les suivants :

- pour les besoins en capacités techniques interministérielles (CTIM) :

- en 2014 : 49,2 M€ en AE et 44,4 M€ en CP ;

- en 2015 : les montants seront révisés dans le cadre du prochain triennal 2015-2017.

- au titre du plan interministériel de modernisation des produits de sécurité gouvernementaux (PMPS) :

- en 2014 : 7,6 M€ en AE et 13 M€ en CP ;

- en 2015 : 16 M€ en AE et 14,9 M€ en CP.

- au titre du programme de chiffreurs lancé en 2012 :

- en 2014 : 2,5 M€ en AE et 3,7 M€ en CP ;

- en 2015 : 1,7 M€ en AE et 1,9 M€ en CP.

- au titre du programme de cryptophonie nouvelle génération (CNG) en cours et des évolutions futures :

- en 2014 : 1,7 M€ d'AE et 8,6 M€ de CP ;

- en 2015 : 1,3 M€ d'AE et 1,9 M€ de CP.

Pour la conduite des autres missions du SGDSN hors ANSSI, l'évolution du budget applique les orientations générales du Gouvernement avec une diminution globale de 15 % à échéance de 2015 par rapport à la loi de finances de 2012.

2. Les effectifs du SGDSN et de l'ANSSI

En 2012 et en 2013, le plafond d'emploi du SGDSN (ANSSI compris) était respectivement de **463 ETPT** et de **531 ETPT** (emplois équivalent temps plein travaillé).

Les effectifs réels du SGDSN et de l'ANSSI au 30 juin 2013 étaient les suivants (y compris les agents mis à disposition) :

EFFECTIFS DU SGDSN ET DE L'ANSSI AU 30 JUIN 2013

Catégorie d'emplois	**Plafond LFI 2013** (en ETPT)	**effectifs SGDSN au 30 juin 2013** (en ETP)	**dont ANSSI** (en ETP)
Catégorie A+	74	46	23
Catégorie A	82	58	25
Catégorie B	40	36	11
Catégorie C	81	97	16
Contractuels	254	293	227
TOTAL	**531**	**530**	**302**

Dans le cadre de la montée en puissance des effectifs de l'agence nationale de la sécurité des systèmes d'information (ANSSI), le SGDSN a obtenu la création de **65 postes supplémentaires** au sein de l'agence en 2013, soit un effectif cible (en ETP) à fin 2013 de **357 agents.**

Les perspectives budgétaires d'emplois pour 2014 et 2015 s'inscrivent, d'une part, dans la montée en puissance des effectifs de l'ANSSI et, d'autre part, dans la réduction des effectifs du SGDSN (hors ANSSI), conformément aux orientations fixées par le Premier ministre (-1 ETP en 2014 et -1 ETP en 2015).

Dans le cadre des travaux sur le Livre blanc sur la défense et la sécurité nationale 2013, le Président de la République a fixé l'objectif d'atteindre un effectif de l'ANSSI de 500 agents à l'horizon 2015. À cet effet, le schéma d'emploi retenu en 2014 pour l'ANSSI est de **+ 65 ETP**, soit une prévision de **422 agents** à échéance de fin 2014.

Comme l'a précisé le Secrétaire général de la défense et de la sécurité nationale, M. Francis Delon, lors de son audition devant la commission *« L'objectif du Livre blanc implique 110 embauches par an, soit le tiers de son effectif. Or la ressource devient rare et chère ; nous avons passé un gentleman agreement avec le ministère de la défense, mais la concurrence avec le secteur privé est ardue. Pourtant la bonne image de l'Anssi lui permet de recruter. Elle embauche en général des jeunes sortis d'école qui iront ensuite irriguer le secteur privé en constituant des relais efficaces de la politique de cybersécurité. »*

Dans ce cadre, les effectifs prévisionnels pour 2014 du SGDSN et de l'ANSSI (en ETP) devraient être les suivants :

EFFECTIFS PRÉVISIONNELS DU SGDSN ET DE L'ANSSI EN 2014

Catégorie d'emplois	**effectifs SGDSN prévisonnels fin 2014** (en ETP)	**dont ANSSI** (en ETP)
Catégorie A+	82	49
Catégorie A	78	44
Catégorie B	50	25
Catégorie C	85	16
Contractuels	334	288
TOTAL	**629**	**422**

Les plafonds d'emploi prévisionnels du SGDSN (ANSSI comprise), à structure constante 2014, s'élèveraient donc à **595 ETPT en 2014** et **627 ETPT en 2015.**

Il convient de rappeler qu'à l'occasion de l'examen du projet de loi de programmation militaire et à l'initiative de vos deux co-rapporteurs pour avis, un amendement a été adopté par le Sénat à la LPM prévoyant d'inscrire, dans la partie du rapport annexé au projet de loi, que :

« les moyens dévolus à la cyberdéfense feront l'objet d'un renforcement significatif. Les ressources humaines seront accrues grâce à un plan de renforcement substantiel concernant notamment plusieurs centaines de spécialistes. En particulier, les effectifs de l'Agence nationale de la sécurité des systèmes d'information, qui devront atteindre 500 agents en 2015, seront régulièrement augmentés, à la hauteur des efforts consacrés par nos principaux partenaires européens. Les moyens du ministère de la défense consacrés à la cyberdéfense poursuivront les montées en puissance décidées antérieurement avec le recrutement d'au moins 350 personnels supplémentaires sur la période 2014-2019 ».

En effet, compte tenu du contexte général de diminution des effectifs et des moyens consacrés à la défense, il a semblé utile à vos deux co-rapporteurs pour avis d'inscrire dans la loi des chiffres précis concernant le renforcement des effectifs consacrés à la cyberdéfense, tant au sein de l'ANSSI qu'au sein des armées et de la direction générale de l'armement.

3. Ce renforcement indispensable reste modeste au regard des moyens consacrés par nos principaux partenaires et alliés

Nos principaux partenaires et alliés ont une organisation sensiblement différente de la nôtre en matière de cyberdéfense.

La comparaison des effectifs affectés à des missions de défense et de sécurité des systèmes d'information est donc délicate.

Il est néanmoins possible de retenir les éléments suivants :

• le *Bundesamt für Sicherheit in der Informationstechnik* (BSI) allemand, dont des missions recouvrent celles de l'ANSSI, a actuellement un effectif de **550 ETP**. Le budget du BSI est comparable à celui de l'ANSSI ;

• la récente réorganisation ayant eu lieu au Royaume-Uni rend plus difficile l'identification du nombre d'effectifs dédiés à des missions comparables. **700 personnes** évoluaient au sein du *Communications Electronics Security Group* (CESG) dont la mission recouvrait une partie de celles de l'ANSSI avant cette réorganisation. Le budget afférent est intégré dans celui consacré au renseignement ;

• pour des missions opérationnelles en partie comparables à celles du centre opérationnel de l'ANSSI, le *Department of Homeland Security* américain, en charge notamment des opérateurs d'importance vitale en dehors du secteur de la sécurité nationale, a un objectif de 1000 collaborateurs. Mais la principale agence en charge de la cyberdéfense aux Etats-Unis est la *National Security Agency* (NSA) dont les effectifs ne sont pas connus mais qui comprend probablement plusieurs milliers d'agents dédiés aux opérations défensives.

II. LES AUTRES CRÉDITS DU PROGRAMME QUI CONCERNENT LES ASPECTS DE DÉFENSE ET DE SÉCURITÉ

Deux instituts placés sous la tutelle du SGDSN relèvent de l'action 2 du programme 129 : l'Institut des hautes études de défense nationale (IHEDN) et l'Institut national des hautes études de la sécurité et de la justice (INHESJ).

Par ailleurs, cette action contient la dotation en fonds spéciaux des services spécialisés de renseignement.

A. L'INSTITUT DES HAUTES ÉTUDES DE DÉFENSE NATIONALE (IHEDN)

L'Institut des hautes études de défense nationale est un établissement public placé sous la tutelle du SGDSN. Il a pour mission de développer l'esprit de défense et de sensibiliser aux questions internationales. A ce titre :

- il réunit des responsables de haut niveau appartenant à la fonction publique civile et militaire ainsi qu'aux différentes catégories socio-professionnelles de la Nation, des Etats-membres de l'Union européenne ou d'autres Etats, en vue d'approfondir en commun leurs connaissances des questions de défense, de politique étrangère, d'armement et d'économie de défense ;

- il prépare à l'exercice de responsabilités de cadres supérieurs militaires et civils, français ou étrangers, exerçant leur activité dans le domaine de la défense, de la politique étrangère, de l'armement et de l'économie de défense ;

- il contribue à promouvoir et à diffuser toutes connaissances utiles en matière de défense, de relations internationales, d'armement et d'économie de défense.

Un contrat de performance pour la période 2011-2013 a pris la suite d'un précédent contrat d'objectifs et de moyens. Il fixe à l'IHEDN des objectifs stratégiques en vue d'une performance accrue des actions de formation, de sensibilisation et de rayonnement que mène l'Institut. Ces objectifs sont maintenus en 2014, avant la signature d'un nouveau contrat couvrant la période triennale 2015-2017.

Dans le cadre du projet de loi de finances pour 2014, l'IHEDN devrait bénéficier d'une subvention pour charge de service public de **8,545 millions d'euros**, contre 8,795 millions d'euros en 2013 et 8,814 millions d'euros en 2012.

La subvention respecte les directives de la lettre de cadrage du budget triennal 2013-2015, ce qui se traduira par une diminution (à périmètre

constant) par rapport à la LFI 2012 de 2,9 % du montant 2015 de la subvention pour charge de service public de l'opérateur.

Compte tenu du rôle important joué par l'IHEDN pour la promotion de l'esprit de défense et le lien Armée-Nation, notamment auprès de la jeunesse, qui ont été rappelés encore récemment par le Président de la République et par le Premier ministre, ainsi qu'en matière de rayonnement international, vos Rapporteurs pour avis regrettent cette diminution de la dotation de l'IHEDN.

La subvention prévue par le PLF 2014 intègre une mesure d'économie supplémentaire induite par la démarche engagée dans le cadre du plan ministériel de modernisation et de simplification, adopté le 8 juillet 2013 par le Premier ministre, qui vise à renforcer les synergies et les mutualisations entre l'IHEDN et l'INHESJ, établissements de formation co-localisés à l'Ecole militaire.

Par rapport au montant prévu au budget triennal 2013-2015, la subvention pour charges de service public de l'IHEDN en 2014 intègre deux mesures supplémentaires :

- une économie de dépense de personnel de 0,1 million d'euros correspondant à la suppression à mi-année de quatre emplois au coût moyen constaté en 2012, s'ajoutant à celle prévue dans le cadre du budget triennal (suppression de deux emplois) ;

- une mesure de transfert de 0,03 million d'euros permettant l'intégration dans la subvention pour charges de service public de la subvention complémentaire annuelle versée par le SGDSN destinée au financement des travaux de doctorants par l'IHEDN.

Les autres ressources en provenance de l'Etat comprennent :

- des sessions nationales « armement et économie de défense » et formations transférées, auparavant réalisées par le centre des hautes études de l'armement (CHEAr), qui feront l'objet en 2014, comme les années précédentes, d'une facturation au ministère de la défense (0,1 million d'euros) à défaut de ressource correspondante intégrée dans la subvention pour charges de service public lors de la fusion en 2010 ;

- des formations spécifiques pour le compte du ministère de la défense (0,1 million d'euros) et du ministère des affaires étrangères (0,5 million d'euros).

BUDGET PRÉVISIONNEL 2013 DE L'IHEDN (EN MILLIERS D'EUROS)

Charges	Compte financier 2012	Budget prévisionnel 2013	Produits	Compte financier 2012	Budget prévisionnel 2013
Personnel	7 699	7 533	Ressources de l'Etat	8 900	8 691
dont charges de pensions civiles	*1 735*	*1 754*	*Subvention de l'Etat*	8 814	8 601
Fonctionnement	2 976	2 805	*Ressources fiscales*	86	90
Intervention			Autres subventions		
			Ressources propres et autres	1 835	2 087
Total des charges	**10 675**	**10 338**	**Total des produits**	**10 735**	**10 778**
Résultat : bénéfice	60	440	Résultat : perte		
Total	**10 735**	**10 778**	**Total**	**10 735**	**10 778**

Source : PAP

Le budget prévisionnel 2013 initial s'élevait à 10,4 millions d'euros. Il a fait l'objet d'un budget rectificatif afin de prendre en compte :

- une mise en réserve complémentaire de 0,4 million d'euros ;

- une augmentation des prévisions de recettes de 0,3 million d'euros.

La prévision de ressources pour 2013 atteint donc 10,8 millions d'euros. Elle comprend :

- la subvention pour charges de service public d'un montant de 8,6 millions d'euros ;

- des ressources fiscales (taxe d'apprentissage) pour un montant de 0,1 million d'euros ;

- des ressources propres pour un montant de 2,1 millions d'euros comprenant :

  - des financements de formation en provenance de services de l'Etat (0,9 million d'euros) ;

- le produit des ventes de prestations de formation, notamment auprès d'auditeurs du secteur industriel (0,8 million d'euros) ;
- d'autres produits de gestion courante et des produits exceptionnels (0,4 million d'euros).

La prévision de dépenses 2013 comprend :

- des rémunérations et charges sociales (7,4 millions d'euros) et des indemnités d'enseignement des conférenciers et vacataires (0,1 million d'euros) pour un montant total de dépenses de personnel de 7,5 millions d'euros ;

- des dépenses de fonctionnement pour un montant de 2,8 millions d'euros, dont 0,8 million d'euros de charges fixes et 2 millions d'euros de charges variables.

En 2013, l'IHEDN compte 107 personnels, dont 104 emplois sous plafond rémunérés par l'opérateur et 3 emplois en fonction rémunérés par l'Etat par d'autres programmes.

Pour 2014, l'IHEDN devrait compter 100 emplois (ETPT) rémunérés par l'opérateur, auxquels s'ajoutent 3 emplois en fonction rémunérés par d'autres programmes, soit au total **103 personnels.**

Le plafond d'emplois pour 2014 intègre **la suppression de 4 ETP.**

Les 3 emplois en fonction à l'Institut rémunérés par d'autres ministères sont :

- le directeur de l'IHEDN (officier général) rémunéré par le ministère de la défense ;

- le directeur-adjoint, secrétaire général (préfet) rémunéré par le ministère de l'intérieur ;

- le directeur-adjoint, chef du département des activités internationales (ministre plénipotentiaire) rémunéré par le ministère des affaires étrangères.

B. L'INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE (IHNESJ)

Établissement public créé par le décret du 28 octobre 2009 et placé sous la tutelle du SGDSN, l'Institut national des hautes études de la sécurité et de la justice (INHESJ) s'est affirmé comme l'opérateur public de référence en ce qui concerne la formation et la recherche liées à la sécurité nationale et à la justice.

L'INHESJ accueille également en son sein l'Observatoire national de la délinquance et des réponses pénales (ONDRP) qui est l'un de ses départements. Les travaux de l'ONDRP sont réalisés avec l'appui de l'INSEE

et font l'objet de plusieurs publications, dont un rapport annuel sur la criminalité en France.

Dans le cadre du contrat d'objectifs et de performance en cours (2011-2013), l'INHESJ s'attache à mettre en œuvre les cinq grands objectifs suivants :

- assurer la qualité de la formation ;

- détecter et réunir les compétences ;

- promouvoir une communauté dynamique de la sécurité et de la justice ;

- mutualiser les champs, missions et moyens ;

- garantir la qualité administrative et budgétaire.

Dans le cadre du projet de loi de finances pour 2014, l'INHESJ devrait bénéficier d'une subvention pour charges de service public de **9,409 millions d'euros.** En 2013, la subvention pour charges de service public était de 9,405 millions d'euros.

Comme pour l'IHEDN, la subvention de l'INHESJ respecte les directives de la lettre de cadrage du budget triennal 2013-2015, ce qui se traduira par une diminution (à périmètre constant) par rapport à la LFI 2012 de 2,9 % du montant 2015 de la subvention.

La subvention prévue par le PLF 2014 intègre une mesure d'économie supplémentaire induite par la démarche engagée dans le cadre du plan ministériel de modernisation et de simplification adopté le 8 juillet 2013 par le Premier ministre qui vise à renforcer les synergies et les mutualisations entre l'IHEDN et l'INHESJ, co-localisés à l'Ecole militaire.

De la même manière que pour l'IHEDN, vos Rapporteurs pour avis regrettent cette diminution de la subvention de l'INHESJ. S'ils estiment nécessaire le renforcement des synergies et des mutualisations entre les deux établissements, co-localisés à l'Ecole militaire, ils considèrent toutefois que ce renforcement ne peut aller jusqu'à une fusion et doit respecter l'identité et la vocation propre de chacun des deux instituts qui ne remplissent pas les mêmes fonctions et ne s'adressent pas aux mêmes publics.

Par rapport au montant prévu dans le budget triennal 2013-2015, la subvention pour charge de service public de l'INHESJ intègre deux mesures supplémentaires :

- une économie de dépense de personnel de 0,1 million d'euros correspondant à la suppression de deux emplois, s'ajoutant à celle prévue dans le cadre du budget triennal (suppression de quatre emplois) ;

- une mesure nouvelle de 0,2 million d'euros permettant de prendre en charge l'augmentation annoncée par l'INSEE de la facture de l'enquête de victimisation entre 2013 et 2014.

Le montant pour 2014 de la subvention pour charges de service public sera ajusté, comme chaque année, avec le reversement au ministère de la défense évalué à 1,2 million d'euros, correspondant au produit annuel de sous-location de l'immeuble de Saint-Denis, pour le financement des travaux de rénovation du bâtiment 13 de l'Ecole militaire, futur siège de l'INHESJ.

L'INHESJ dispose de ressources propres provenant des droits d'inscription aux différents programmes de formation dispensés par l'institut ainsi que par le financement de plusieurs programmes de recherche. Les autres ressources propres sont issues des produits de sous-location des locaux de l'immeuble Les Borromées (Plaine Saint-Denis), précédente implantation prise à bail par l'institut avant son déménagement à l'Ecole militaire.

BUDGET PRÉVISIONNEL 2013 DE L'INHESJ (EN MILLIERS D'EUROS)

Charges	Compte financier 2012	Budget prévisionnel 2013	Produits	Compte financier 2012	Budget prévisionnel 2013
Personnel	5 994	6 057	Ressources de l'Etat	7 756	9 157
dont charges de pensions civiles	*1 019*	*1 030*	*Subvention de l'Etat*	7 732	9 137
Fonctionnement	4 738	4 675	*Ressources fiscales*	24	20
Intervention			Autres subventions		70
			Ressources propres et autres	3 157	3 205
Total des charges	**10 732**	**10 732**	**Total des produits**	**10 913**	**12 432**
Résultat : bénéfice	181	1 700	Résultat : perte		
Total	**10 913**	**12 432**	**Total**	**10 913**	**12 432**

Source : PAP

En 2013, l'INHESJ compte 89 personnels dont 83 emplois sous plafond, rémunérés par l'opérateur, et 6 emplois en fonction, rémunérés par l'Etat, par d'autres collectivités ou organismes.

Pour 2014, l'INHESJ devrait compter 80 emplois rémunérés par l'opérateur dont 79 sous plafond et un poste hors plafond, auxquels s'ajoutent 5 emplois en fonction, soit au total **85 personnels.**

Le plafond d'emplois pour 2014 intègre **la suppression de 4 ETP.** Un emploi hors plafond recruté en 2013 est chargé d'études sur un projet de recherche financé par l'agence nationale de la recherche.

Les 3 emplois en fonction à l'Institut rémunérés par d'autres ministères sont :

- le directeur de l'INHESJ (inspecteur général de la police nationale) rémunéré par le ministère de l'intérieur ;

- un chargé de mission « sécurité sanitaire » (inspecteur des services vétérinaires) rémunéré par le ministère de l'agriculture ;

- un chargé de mission « douanes » à l'ONDRP rémunéré par le ministère de l'économie et des finances.

Les deux emplois en fonction à l'Institut rémunérés par des collectivités locales concernent les postes d'officiers de sapeurs-pompiers mis à disposition de l'INHESJ contre remboursement.

C. LES FONDS SPÉCIAUX

Une dotation de **50,2 millions d'euros** en autorisations d'engagement et de crédits de paiement est destinée aux fonds spéciaux. Il est habituel que des abondements de crédits interviennent en gestion.

Les fonds spéciaux sont destinés aux services de renseignement, principalement la Direction générale de la sécurité extérieure (DGSE), ainsi qu'au Groupement interministériel de contrôle (GIC), organisme rattaché au Premier ministre, chargé des interceptions de sécurité.

L'utilisation des fonds spéciaux fait l'objet d'un contrôle par la Commission de vérification des fonds spéciaux, qui est chargée de vérifier, en application de l'article 154 de la loi de finances pour 2002 du 28 décembre 2011, que les crédits affectés aux fonds spéciaux ont été utilisés conformément à leur destination.

Dans le cadre du projet de loi de programmation militaire, il est prévu une absorption de la Commission de vérification des fonds spéciaux par la Délégation parlementaire au renseignement, ce qui devrait permettre de renforcer le contrôle parlementaire sur les services de renseignement.

EXAMEN EN COMMISSION

La commission a examiné le présent rapport pour avis lors de sa réunion du 19 novembre 2013.

M. Jacques Berthou, rapporteur pour avis. – Nous souhaiterions vous présenter, avec notre collègue M. Jean-Marie Bockel, les principales lignes directrices du programme 129 « coordination du travail gouvernemental » dans le cadre de l'examen du projet de loi de finances pour 2014.

Comme vous le savez, c'est la première fois que notre commission se prononce par un avis budgétaire sur ce programme de la mission « Direction de l'action du Gouvernement », qui relève du Premier ministre.

Or, ce programme comprend pour une grande part des crédits qui intéressent directement la défense et la sécurité nationale, comme ceux du Secrétariat général de la défense et de la sécurité nationale (SGDSN), de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), mais aussi de l'Institut des hautes études de la défense nationale (IHEDN) et de l'Institut national des hautes études de la sécurité et de la justice (INHESJ).

Il était donc important que notre commission, notamment dans le prolongement de nos travaux sur la cyberdéfense, se prononce par un avis sur ce budget et nous voudrions remercier la commission et son président de nous avoir désignés comme rapporteurs pour avis sur ce programme.

Pour étudier ce budget, nous avons auditionné, en commission, M. Francis Delon, Secrétaire Général de la défense et de la sécurité nationale. Nous avons également rencontré M. Patrick Pailloux, directeur général de l'ANSSI, ainsi que M. Alain Juillet, ancien délégué interministériel à l'intelligence économique et le responsable de la sécurité d'EDF, M. Espagnol.

Je vous présenterai brièvement les priorités et les crédits du programme 129 et ceux du SGDSN, avant de laisser la parole à notre collègue M. Jean-Marie Bockel, pour qu'il vous présente les crédits de l'ANSSI ainsi que ceux de l'IHEDN et de l'INHESJ.

Dans le cadre du projet de loi de finances pour 2014, le budget du SGDSN devrait être de 191 millions d'euros en autorisations d'engagement et de 193 millions d'euros en crédits de paiement. Les effectifs devraient passer de 530 agents en 2013 à 595 agents en 2014, principalement au profit de l'Agence nationale de la sécurité des systèmes d'information. Hors ANNSI, le SGDSN compte environ 200 agents.

Enfin, le programme comprend les crédits des fonds spéciaux, à hauteur de 49,7 millions d'euros.

Je rappelle que ces crédits, qui sont principalement destinés aux services de renseignement, font l'objet d'un contrôle de la commission de vérification des fonds spéciaux, au sein de laquelle siègent deux députés et

deux sénateurs, le Président de notre commission et notre collègue M. André Dulait.

M. Jean-Marie Bockel, rapporteur pour avis. – J'en viens maintenant aux crédits et aux effectifs de l'Agence nationale de la sécurité des systèmes d'information (l'ANSSI).

Comme vous le savez, nous avions regretté dans notre rapport d'information sur la cyberdéfense, adopté en juillet 2012, la faiblesse des moyens et des effectifs consacrés en France à la cyberdéfense, notamment par rapport à ceux de nos principaux partenaires européens, et l'une de nos principales recommandations visait à augmenter les moyens et les effectifs de l'ANSSI.

Je rappelle, en effet, qu'avec un budget de 70 millions d'euros et des effectifs de 350 agents en 2013, les moyens de l'ANSSI restent encore très inférieurs à ceux dont disposent nos partenaires britannique ou allemand, qui sont de deux à trois fois supérieurs.

Or, l'actualité (avec notamment les révélations sur l'ampleur de l'espionnage informatique américain) ne cesse de nous rappeler l'importance d'assurer la protection des systèmes d'information les plus sensibles face aux attaques informatiques. Cela vaut naturellement pour l'Etat mais aussi pour les opérateurs d'importance vitale, comme l'énergie ou les transports.

Dans notre rapport, nous avions donc « tiré la sonnette d'alarme », mais il me semble que cet appel a été entendu et que nous progressons dans la bonne direction, même si naturellement il reste encore beaucoup à faire.

La cyberdéfense a été consacrée comme l'une des premières priorités dans le cadre du nouveau Livre blanc et de la Loi de programmation militaire.

Dans ce cadre, il est prévu une augmentation régulière des effectifs et des moyens de l'ANSSI, des armées et de la DGA consacrés à la cyberdéfense. En particulier, le nouveau Livre blanc et le projet de LPM prévoient que les effectifs de l'ANSSI devraient atteindre 500 agents à l'horizon 2015, conformément à l'engagement du Président de la République. Dans le cadre du projet de loi de finances pour 2014, l'ANSSI devrait donc bénéficier de la création de 65 postes supplémentaires et d'une augmentation de son budget de 20 %.

Parallèlement, la LPM prévoit un effort de 350 personnels et de 360 millions d'euros supplémentaires pour la cyberdéfense dans les armées sur la période 2014-2019, ainsi qu'une augmentation des effectifs de la DGA et un triplement des crédits consacrés à la recherche qui devraient atteindre 30 millions d'euros par an.

En outre, l'ANSSI et le centre cyber des armées sont co-localisés depuis cette année dans l'immeuble « Tour Mercure ».

Je me félicite donc que nos préconisations aient été suivies d'effets, malgré un contexte budgétaire difficile et un vivier de recrutement assez limité en raison du manque d'ingénieurs.

Enfin, je conclurai notre intervention par la présentation de deux instituts qui relèvent de ce programme : l'Institut des hautes études de défense nationale (IHEDN) et l'Institut national des hautes études de la sécurité et de la justice (INHESJ).

L'IHEDN est un établissement public administratif chargé d'aider les cadres de la Nation à se forger une perception de la défense, à développer une sensibilité à ses enjeux et à acquérir une culture de défense. L'Institut organise des formations – au niveau national et régional et à l'international – destinée à un public français et étranger et joue un rôle important pour promouvoir l'esprit de défense.

L'INHESJ a pour mission d'intervenir dans la formation, des études, de la recherche, de la veille et de l'analyse stratégique en matière de sécurité intérieure, ainsi que dans ceux intéressant la justice et les questions juridiques.

Dans le cadre du projet de loi de finances pour 2014, l'IHEDN bénéficie d'une subvention pour charges de service public de 8,6 millions d'euros (contre 8,8 en 2013) et l'INHESJ d'une subvention de 9,4 millions d'euros. Ces subventions sont en diminution par rapport à 2013. Le nombre d'emplois passe de 104 en 2013 à 100 en 2014 pour l'IHEDN, soit une suppression de 4 postes, et de 83 à 79 pour l'INHESJ, soit 4 postes en moins.

Compte tenu du rôle important joué par ces deux instituts, notamment en termes de rayonnement à l'international, je regrette personnellement cette diminution des moyens.

Ces diminutions devraient toutefois être compensées par un renforcement des mutualisations et des synergies entre les deux établissements co-localisés à l'Ecole militaire, et qui sont placés sous la tutelle du SGDSN.

M. Jean-Louis Carrère, président. – Je remercie les deux rapporteurs pour avis de leur présentation et je me félicite que les préconisations de notre commission aient été suivies d'effets, notamment en ce qui concerne l'augmentation des effectifs et du budget de l'ANSSI.

M. André Dulait. – Etant donné que cette augmentation des moyens consacrés à la cyberdéfense correspond à une forte demande exprimée par notre commission dans ses précédents rapports présentés par notre ancien collègue Roger Romani en 2008 puis par notre collègue Jean-Marie Bockel en 2012, il serait incohérent de refuser de voter les crédits prévus par ce programme.

Sur proposition de ses deux rapporteurs pour avis, la commission donne à l'unanimité un avis favorable à l'adoption des crédits de la mission « Direction de l'action gouvernementale ».

ANNEXE I - AUDITION DE M. FRANCIS DELON, SECRÉTAIRE GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Lors de sa séance du 23 octobre, la commission a auditionné M. Francis Delon, secrétaire général de la défense et de la sécurité nationale.

M. Daniel Reiner, président. - Deux jours après l'approbation par le Sénat de la loi de programmation militaire, à laquelle vous avez beaucoup oeuvré, je peux vous exprimer la satisfaction du Sénat d'avoir mené à bien un débat de qualité et où tous les acteurs étaient de bonne foi. Nous avons adopté des amendements ayant une forte valeur symbolique, visant essentiellement la sécurisation financière, mais aussi renforçant les pouvoirs de contrôle des parlementaires. Avec Xavier Pintat et Jacques Gautier, nous avons été au fond de la question ; nous avons même remis autour de la table des gens qui ne se parlaient plus, mais certains refus incompréhensibles nous ont agacés.

Nous vous entendons aujourd'hui sur les crédits pour 2014 du Secrétariat général de la défense et de la sécurité nationale (SGDSN), sur lesquels nous donnons un avis par la voix de deux rapporteurs : Jacques Berthou et Jean-Marie Bockel. Le positionnement du budget de votre service - rattaché au premier ministre - au sein du programme 129 « Coordination de l'action gouvernementale » de la mission « Direction de l'action du gouvernement » explique que nous l'étudiions pour la première fois. Cette mission faisait l'objet d'un rapport au fond de la commission des finances et le programme 129 d'un rapport pour avis de la commission des lois. Or de nombreuses compétences du SGDSN concernent directement la défense : la lutte contre la prolifération, l'exportation de matériel de guerre, la planification en fait de défense et sécurité, l'entrainement et la préparation à la gestion de crises graves, la protection du secret de la défense nationale, la sécurité des communications gouvernementales, des systèmes d'informations et la cyberdéfense.

M. Francis Delon, secrétaire général de la défense et de la sécurité nationale. - Le SGDSN avait préparé le Livre blanc par un document d'orientation stratégique dès la fin de l'année 2011 ; il a participé à l'élaboration du Livre blanc et au projet de loi de programmation militaire. Cette activité intense s'est ajoutée aux missions générales et quotidiennes du SGDSN au service du Président de la République et du premier ministre sur l'ensemble des sujets relevant de la sécurité nationale et de la défense. La croissance exponentielle du nombre d'intrusions informatiques contre les infrastructures nationales a conduit le Gouvernement en 2009 à créer une agence nationale de la sécurité des systèmes d'information (Anssi) qui m'est rattachée et est chargée de répondre aux attaques contre les administrations

de l'État, mais aussi désormais contre les opérateurs d'importance vitale (OIV) et les entreprises indispensables à notre stratégie de sécurité nationale.

Le SGDSN est structuré autour de deux directions consacrées d'une part à la protection et à la sécurité de l'État (PSE) et d'autre part aux affaires internationales, stratégiques et technologiques (AIST). Elle comporte une agence, l'Anssi et assure la tutelle de deux établissements publics de formation : l'institut des hautes études de défense nationale (IHEDN) et l'institut national des hautes études de la sécurité et de la justice (INHESJ).

Le SGDSN est d'abord un outil au service du gouvernement pour le traitement des sujets sensibles en matière de défense et de sécurité nationale. Il assure ainsi le secrétariat du Conseil de défense et de sécurité dans toutes ses formations. Cette instance présidée par le Président de la République est compétente sur la programmation militaire, la politique de dissuasion, la programmation de sécurité intérieure, la sécurité économique et énergétique, la lutte contre le terrorisme ou la planification de réponse aux crises. Au cours des douze derniers mois, elle a notamment préparé les travaux permettant de valider le Livre blanc de la défense et de la sécurité nationale et le projet de loi de programmation militaire. Ce conseil dans sa formation restreinte a examiné les orientations à prendre pour la conduite des crises diverses, comme celles du Mali, de la Syrie ou de la République centrafricaine. Il comporte deux formations spécialisées qui traitent de sujets spécifiques avec une composition adaptée : le Conseil des armements nucléaires et le Conseil national du renseignement.

Le SGDSN dispose d'une capacité d'analyse et de synthèse, de veille, d'alerte et d'appui à la décision relatives aux questions de sécurité internationale afin de répondre à des demandes du cabinet du Premier ministre ou de la présidence de la République. Sa direction AIST suit les conflits et les crises internationales susceptibles d'affecter les intérêts français, en particulier ceux dans lesquels nos forces sont engagées et anime des groupes interministériels d'analyse sur des sujets tels que les crises affectant le monde arabe, l'Iran ainsi que les zones sahélo-saharienne et afghano-pakistanaise. En fonction de l'actualité, elle peut être sollicitée pour produire des synthèses sur l'évolution de la situation de certains théâtres d'opération, comme depuis janvier 2013 avec la diffusion régulière d'une synthèse de la situation au Sahel. Elle assure la coordination interministérielle sur des questions d'ordre stratégique, telles que le terrorisme, la défense anti-missiles balistiques, le développement du recours aux entreprises de services de sécurité et de défense, la protection des navires dans les zones à risques. Elle est chargée sur ces dossiers de proposer au Président de la République et au gouvernement des orientations et arbitrages.

Le SGDSN assure aussi une veille scientifique et technique permanente dans les domaines nucléaire, radiologique, biologique, chimique et relatif aux explosifs (NRBCE), ainsi que dans le domaine des missiles et le

domaine spatial. Il coordonne ou concourt activement aux actions interministérielles portant sur la lutte contre la prolifération, la protection du potentiel scientifique et technique de la Nation, la sécurité du programme européen de navigation par satellite Galileo et le contrôle des images spatiales. Il coordonne des études en matière de lutte contre la prolifération des armes de destruction massive et de leurs vecteurs et produit des documents de synthèse sur les dossiers d'actualité, tels que l'Iran, la Syrie et la Corée du nord. Il assure le secrétariat du comité interministériel pour l'application de la convention sur l'interdiction des armes chimiques (Ciac) et coordonne les travaux portant sur la biologie de synthèse. Il coordonne la réponse nationale à l'initiative internationale Proliferation Security Initiative (PSI), consistant à échanger entre pays membres des informations sur des transits par voie maritime de cargaisons proliférantes et à faciliter leur interception. Celles-ci se multiplient : huit affaires d'interception de biens proliférants ont été menées dans ce cadre depuis l'été 2012.

La France dispose d'une importante base industrielle et technologique de défense qui contribue à la préservation de notre souveraineté, participe à la croissance économique et représente des dizaines de milliers d'emplois. L'exportation de matériels de guerre est soumise à une procédure d'autorisation préalable par décision du Premier ministre - ou du SGDSN par délégation - après avis de la commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG), dont le SGDSN assure le secrétariat tout en construisant une doctrine dans ce domaine. Le dispositif de contrôle des exportations de matériels de guerre découlant de la loi du 22 juin 2011 évolue : l'année prochaine, un système simplifié de licence unique d'exportation et de transferts intracommunautaires remplacera le mécanisme actuel. Par ailleurs et conformément aux conclusions du Livre blanc de 2013, le SGDSN contribue à une réflexion plus générale sur le renforcement du contrôle des exportations de biens et technologies à double usage et participe à la totalité des commissions interministérielles des biens à double usage (CIBDU). La France a obtenu, dans le cadre de l'arrangement de Wassenaar, que les outils de surveillance et de contrôle de l'internet soient soumis à autorisation avant leur exportation, comme les matériels d'interception des communications téléphoniques mobiles depuis 2011.

Le SGDSN contribue ensuite à la politique de sécurité nationale. Il procède à la rénovation des plans de protection de la famille Pirate - dont le plan Vigipirate de lutte contre le terrorisme - dans la continuité du travail engagé en 2012, pour aboutir fin 2013 à un nouveau plan Vigipirate qui gardera les principes qui font la force du plan actuel mais qui sera rendu plus efficace par une meilleure visibilité. Une grande partie du plan, aujourd'hui classifié, devrait ainsi être rendue public. Le pilotage des postures de protection sera également amélioré par une caractérisation plus fine des menaces terroristes et des vulnérabilités. Dans les deux ans à venir, les autres plans d'intervention de la famille Pirate - Pirate-air, Pirate-mer, Piranet - seront révisés, à l'exception du plan NRBC qui date de 2011.

Le premier ministre a confié en août dernier au SGDSN une mission relative à la mise en œuvre d'une stratégie nationale de prévention de la radicalisation, visant à identifier et réduire les vulnérabilités des individus et des groupes face aux idées radicales de toute nature pouvant déboucher sur l'action violente. Lancés début septembre, les travaux associent l'ensemble des ministères concernés et permettent une analyse des dispositifs existants en les comparant avec les initiatives étrangères.

L'organisation gouvernementale de gestion de crise a été consolidée ; la professionnalisation de ses acteurs a été engagée depuis 2012 par des exercices majeurs rénovés et des entrainements spécifiques permettant de former les personnels armant la cellule interministérielle de crise (CIC). Les premiers effets positifs de ce programme global de professionnalisation ont pu être mesurés lors des derniers exercices majeurs, ainsi qu'au travers du bon fonctionnement de la CIC lors des dernières crises, à l'exemple de l'épisode neigeux de l'hiver 2012-2013. Le SGDSN a poursuivi son action de développement d'une culture d'anticipation des crises au sein des ministères.

La gestion de crise s'accompagne d'un renforcement de la résilience qui doit être perçue à la fois comme un objectif (renforcer la cohésion et la solidité de la Nation face aux risques et menaces) et comme une méthode (mobiliser tous les acteurs). Pour atteindre ce double objectif, le SGDSN a initié en 2012 les travaux visant à instaurer une politique nationale de résilience qui s'appuie sur le dispositif de sécurité des activités d'importance vitale, ainsi que sur des actions complémentaires permettant d'améliorer la continuité des activités indispensables à la nation. Il a ainsi publié un guide d'aide à l'élaboration des plans de continuité d'activité à destination des administrations, des collectivités et des entreprises.

Le contrat général interministériel créé par le Livre blanc déterminera, dans une perspective de programmation budgétaire, les capacités critiques des ministères civils et leur niveau d'engagement dans la réponse aux crises majeures. Cette démarche sera prolongée à l'horizon 2016 sous l'autorité du ministre de l'intérieur par une planification territoriale.

Le SGDSN a préparé la mise en place du comité de la filière industrielle de sécurité (Cofis), qu'installera ce soir le Premier ministre. Rassemblant onze ministres, vingt et un présidents-directeurs généraux de sociétés, cinq présidents de groupements industriels et dix-neuf personnalités qualifiées, dont des représentants de la recherche académique, la présidente de la commission informatique et liberté (Cnil) et plusieurs parlementaires, le Cofis définira les besoins et les orientations de la filière : à la différence de l'industrie de défense, qui n'a qu'un seul client, l'État, l'industrie de la sécurité n'a jamais fait l'objet d'une planification. Nos forces font dès lors leurs achats bien souvent sur étagère, et parfois au profit de fournisseurs étrangers.

Le Livre blanc sur la défense et la sécurité nationale marque une nouvelle étape dans la prise en compte par les pouvoirs publics des questions liées à la cybersécurité. La France doit faire face à l'espionnage et au sabotage - encore peu présent, mais auquel il faut se préparer. Les dispositions de la loi de programmation militaire font écho à cette préoccupation.

L'Anssi, quant à elle, a la responsabilité de conduire ou de coordonner l'ensemble des actions destinées à prévenir les attaques contre les systèmes d'information et à réagir en cas d'atteinte à leur disponibilité ou à leur intégrité. Son action s'exerce principalement au profit de l'État, mais également des opérateurs d'importance vitale du secteur public et privé. Elle est chargée, dans son champ de compétences, d'élaborer la stratégie de l'État et de développer et d'entretenir la coopération internationale. Cette stratégie nationale partiellement couverte par le secret de la défense nationale se fixe pour objectifs la protection de l'information de souveraineté de l'État, la sécurisation des systèmes d'information des entreprises les plus sensibles et le positionnement de la France comme nation majeure en matière de cyberdéfense. Elle protège ainsi les systèmes d'information de l'État et des OIV et assure la sécurité des communications du Président de la République et du gouvernement ; elle coordonne l'action gouvernementale en cas d'attaque ou de compromission des systèmes et prend la main en cas d'attaque majeure. Elle donne des instructions aux opérateurs conformément à la loi de programmation militaire et mobilise des groupes d'intervention rapide.

En 2012, l'Anssi a traité 27 cyberattaques majeures visant des administrations ou des grandes entreprises nationales ; ses effectifs étaient insuffisants pour traiter toutes les attaques dont elle a eu connaissance. Elle héberge le centre d'alerte et de réaction aux attaques informatiques (CERT), qui est alerté sur des incidents, analyse les codes malveillants, rédige des synthèses des incidents traités et propose le cas échéant des mesures générales de prévention. Le CERT a reçu en 2012 plus de 700 signalements mais n'a pu - ou pas voulu, car certains s'avèrent anodins - en traiter que 70.

La loi de programmation militaire représente une avancée sur la sécurisation des entreprises appartenant aux secteurs d'activité d'importance vitale. Le renforcement de la sécurité des systèmes d'information passe aussi par la labellisation de produits et de services et par le maintien d'un tissu industriel de confiance. Nous encourageons ainsi des PME, dont certaines sont des perles technologiques en matière de cyberdéfense et auxquelles nous déléguons des activités. L'agence apporte aussi son expertise technique dans le cadre des investissements d'avenir et est consultée par la direction générale du trésor lorsque des demandes d'autorisation d'investissements étrangers concernent des entreprises du secteur de la sécurité des systèmes d'information.

L'Anssi mène une politique de communication de plus en plus active en direction des administrations de l'État, des entreprises et même du grand public. À travers son centre de formation à la sécurité des systèmes d'information (CFSSI), elle forme des acteurs publics à ces questions.

L'accomplissement de l'ensemble de ces missions suppose de disposer de personnels très compétents - c'est le cas - et d'un budget préservé. Ce dernier est globalement de 195 millions d'euros de crédits de paiement, y compris le titre II, dont une soixantaine de millions sont transférés au ministère de la défense pour des projets interministériels. Le budget de l'Anssi bénéficie de la montée en puissance de la politique de lutte contre les cybermenaces, tandis que celui du reste du SGDSN tend plutôt à la baisse. Ce dernier dispose d'un service d'administration générale capable de répondre aux multiples sollicitations liées à la multiplicité des statuts et des personnels militaires ou civils, fonctionnaires ou contractuels, et qui a géré 220 embauches en 2013.

La croissance rapide de l'Anssi implique une augmentation du titre II. Le Livre blanc fixe un effectif cible de 500 agents en 2015 ; le projet de loi de finances prévoit 65 équivalents temps plein supplémentaires en 2014 pour arriver à 422 à la fin de l'année. L'objectif du Livre blanc implique 110 embauches par an, soit le tiers de son effectif. Or la ressource devient rare et chère ; nous avons passé un gentleman agreement avec le ministère de la défense, mais la concurrence avec le secteur privé est ardue. Pourtant la bonne image de l'Anssi lui permet de recruter. Elle embauche en général des jeunes sortis d'école qui iront ensuite irriguer le secteur privé en constituant des relais efficaces de la politique de cybersécurité.

Le SGDSN hors ANSSI, dont les missions ne cessent de s'approfondir et de se renforcer depuis deux Livres blancs, respecte la discipline budgétaire générale et contracte ses effectifs : il comptera 207 agents à la fin de 2014. Il applique les mêmes règles aux établissements placés sous sa tutelle. Il alloue par transfert budgétaire une part importante de son budget d'investissement à des opérations conduites par la Direction générale de la sécurité extérieure (DGSE) ou la DGA. Il est maître d'ouvrage des réseaux de communication gouvernementaux sécurisés. Le renouvellement quasi simultané de l'intranet sécurisé interministériel pour la synergie gouvernementale (ISIS) et du réseau interministériel de base uniformément durci (RIMBAUD) devrait donner lieu à des engagements importants en 2016. Au sein du centre de transmissions gouvernemental (CTG), des investissements particuliers couvrent le développement des moyens de communication du Président de la République, notamment le système embarqué dans l'avion à usage gouvernemental. Les plafonds de crédits révisés s'élèvent à 64,1 millions d'euros d'autorisations d'engagement et 70,5 millions d'euros de crédits de paiement. Ils seront ajustés l'année prochaine dans le cadre des travaux sur le budget triennal 2015-2017.

M. Jeanny Lorgeoux. - Malgré les dénégations alambiquées de James Klepper, la pieuvre de la National Security Agency (NSA) a fait la preuve de son efficacité, qui rend diaphane le secret de nos ambassades et de nos administrations. Est-il possible de lutter contre cet espionnage par un pays allié et ami, ou sommes-nous condamnés, tel Sisyphe, à lutter indéfiniment et vainement contre lui ? La loi de programmation militaire comporte un important volet relatif à la cyberdéfense ; ces mesures sont-elles suffisantes ? J'aimerais mesurer le décalage entre nos petits efforts et l'ampleur de la tâche. Je n'ai pu assister au dernier conseil d'administration de l'IHEDN, mais j'ai cru comprendre que son budget avait été raboté de 300 000 euros...

M. Jacques Gautier. - On a pu observer le rôle discret mais essentiel du SGDSN lors de la préparation du Livre blanc. Votre budget peut paraître limité par rapport à celui que nous examinons habituellement ; il n'est pas concerné par la loi de programmation militaire, mais par la loi de finances triennale. Compte tenu du caractère mouvant des questions que vous traitez, seriez-vous favorables à une actualisation tous les deux ans, plutôt que tous les trois ans ? Quels sont vos liens en matière de renseignement avec le coordonnateur du renseignement auprès du Président de la République, et avec le délégué interministériel à l'intelligence économique ? Pour faire face aux réductions de crédits alloués à l'IHEDN et à l'INHESJ, comptez-vous recourir à la mutualisation ou supprimer une session de formation une fois de temps en temps ? L'augmentation du contrôle parlementaire sur les services de renseignement introduit par la loi de programmation militaire semble-t-elle excessive au professionnel que vous êtes ?

M. Francis Delon.- Les menaces qui pèsent sur nos systèmes d'information ne sont pas nouvelles ; le Monde ne nous apprend rien. Pour les prévenir, il nous faut des moyens de détection des attaques et de protection des communications sensibles, mais aussi une discipline dans leur usage, qu'il nous faut rappeler en permanence. Sur ce point, il y a eu des progrès. C'est un combat qui existe dans tous les pays. Les dispositions de la loi de programmation militaire vont dans ce sens. Compte tenu de l'origine de l'espionnage allégué, rapporté par le journal Le Monde, les plus hautes autorités de l'État ont exprimé leur incompréhension et leurs protestations auprès des autorités américaines.

Monsieur Lorgeoux, nous n'avons pas sacrifié en votre absence le budget de l'IHEDN lors du dernier conseil d'administration ! J'ai demandé à l'IHEDN et à l'INHESJ de faire des économies, mais sans réduire leurs missions. Nous nous efforçons de mutualiser les activités matérielles des deux instituts mais nous n'allons pas les fusionner car ils ont leur personnalité propre.

Nos liens avec le coordonnateur national du renseignement sont étroits et nous travaillons sur des sujets thématiques et géographiques. Nos relations avec la déléguée interministérielle à l'intelligence économique sont

excellentes. Je l'ai notamment associée aux travaux sur le comité de filière que j'ai mentionné tout à l'heure.

M. Robert del Picchia. - Je ne vous interrogerai pas sur les cyberattaques. Il y a un an et demi, notre rapport, qui avait déplu au quai d'Orsay, traitait de la fonction anticipation stratégique et soulignait quelques disfonctionnements. La coordination s'est-elle améliorée ? La transmission de l'information fonctionne-t-elle mieux ?

Lors de l'examen de la loi de programmation militaire, la commission des lois souhaitait beaucoup plus d'informations et de transparence en matière de renseignement alors que notre commission estimait que la transparence avait ses limites pour ne pas mettre en danger les personnels. Quelle est votre position ?

M. André Trillard. - Vous avez évoqué la sécurisation des entreprises. Mais où commence l'intérêt national ? Vous limitez-vous aux fournisseurs bien connus des services de l'État ou vous intéressez-vous aussi aux PME ? Si tel est le cas, qui se charge de ces PME ?

Dans certaines administrations, comme les grandes écoles, les grandes universités, le monde de la recherche, la notion de sécurisation en est encore à ses balbutiements : le seul critère retenu semble celui de la gratuité. Quid de la sécurité ?

Dans quels délais accordez-vous des visas pour les exportations de matériel militaire ? Ces délais ont indéniablement un impact économique.

M. Francis Delon. - Le Livre blanc évoque l'anticipation stratégique et prévoit un dispositif plus efficace pour coordonner les actions de la délégation aux affaires stratégiques (DAS) et de la direction générale de l'armement du ministère de la défense, de la direction de la prospective du quai d'Orsay, et de nous-même. Nous allons prochainement réunir tous ces services pour que chacun explique ce qu'il veut faire en matière d'anticipation. Ceci nous permettra de coordonner nos actions et d'éviter les doublons. Nous jugerons de ce travail dans quelques mois, et nous tiendrons compte de vos recommandations.

En ce qui concerne les exportations de matériel de guerre, elles ne peuvent se faire sans autorisation. La commission compétente se réunit une fois par mois et elle examine des centaines d'affaires. Mais tous les jours, avec les ministères de la défense, des affaires étrangères, de l'économie et, parfois, de la recherche, nous examinons des dossiers et décidons sans attendre le rendez-vous mensuel. Nous nous efforçons d'avoir des délais rapides.

M. Daniel Reiner, président. - Les directives communautaires ont permis de simplifier les procédures.

Je vous remercie pour toutes ces informations.

ANNEXE II-
LISTE DES PERSONNES ENTENDUES

Le mercredi 25 septembre 2013 :

M. Patrick PAILLOUX, Directeur général de l'ANSSI et M. Christian DAVIOT, conseiller « stratégie » ;

Contre-Amiral Arnaud COUSTILLIERE, officier général à la cyberdéfense à l'état-major des armées.

Le mercredi 6 novembre 2013 :

M. Alain JUILLET, ancien Délégué interministériel à l'intelligence économique, Président du CDSE (club des directeurs de la sécurité des entreprises) ;

M. Patrick ESPAGNOL, ancien Préfet, Directeur de la sécurité d'EDF.