N° 110

SÉNAT

SESSION ORDINAIRE DE 2014-2015

Enregistré à la Présidence du Sénat le 20 novembre 2014

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* **2015**, *ADOPTÉ PAR L'ASSEMBLÉE NATIONALE,*

TOME IX

DIRECTION DE L'ACTION DU GOUVERNEMENT : COORDINATION DU TRAVAIL GOUVERNEMENTAL

Par MM. Jean-Marie BOCKEL et Jean-Pierre MASSERET,

Sénateurs.

(1) Cette commission est composée de : M. Jean-Pierre Raffarin, *président ;* MM. Christian Cambon, Daniel Reiner, Jacques Gautier, Aymeri de Montesquiou, Mmes Josette Durrieu, Michelle Demessine, MM. Xavier Pintat, Gilbert Roger, Robert Hue, Mme Leila Aïchi, *vice-présidents ;* M. André Trillard, Mmes Hélène Conway-Mouret, Joëlle Garriaud-Maylam, MM. Joël Guerriau, Alain Néri, *secrétaires ;* MM. Michel Billout, Jean-Marie Bockel, Michel Boutant, Jean-Pierre Cantegrit, Bernard Cazeau, Pierre Charon, Robert del Picchia, Jean-Paul Emorine, Philippe Esnol, Hubert Falco, Bernard Fournier, Jean-Paul Fournier, Jacques Gillot, Mme Éliane Giraud, M. Gaëtan Gorce, Mme Nathalie Goulet, M. Alain Gournac, Mme Sylvie Goy-Chavent, MM. Jean-Pierre Grand, Jean-Noël Guérini, Didier Guillaume, Mme Gisèle Jourda, M. Alain Joyandet, Mme Christiane Kammermann, M. Antoine Karam, Mme Bariza Khiari, MM. Robert Laufoaulu, Jacques Legendre, Jeanny Lorgeoux, Claude Malhuret, Jean-Pierre Masseret, Rachel Mazuir, Christian Namy, Claude Nougein, Philippe Paul, Mme Marie-Françoise Perol-Dumont, MM. Cédric Perrin, Jean-Vincent Placé, Yves Pozzo di Borgo, Henri de Raincourt, Alex Türk.

Voir les numéros :

Assemblée nationale (**14**ème législ.) : **2234, 2260** à **2267** et T.A. **420**

Sénat : **107** et **108** à **114** (2014-2015)

SOMMAIRE

Mesdames, Messieurs,

Pour la deuxième année consécutive, 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.

C'est un signal fort de l'importance que revêtent désormais, pour notre défense et notre sécurité nationales, au sein des crédits rattachés au Premier ministre, les crédits consacrés notamment à la gestion des crises, au renseignement et à la cyberdéfense.

Ce rapport est en effet l'occasion 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.

Il permet également, dans le prolongement des travaux passés de votre commission sur la cyberdéfense[1], de suivre attentivement l'évolution des moyens qui y sont consacrés, au travers des dotations et des effectifs de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Il complète, enfin, l'information de la commission sur le suivi des moyens des services de renseignement, notamment au travers des fonds spéciaux destinés aux services de renseignement, qui figurent au sein du programme 129.

Au total, c'est donc près de la moitié du programme 129 qui est directement consacrée à des actions touchant la sécurité nationale et la défense, à **l'action 2 « Coordination de la sécurité et de la défense »** dotée de **261 millions d'euros** en autorisations d'engagement et **293 millions d'euros** de crédits de paiement en 2015.

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) ;

[1] *« La cyberdéfense, un enjeu mondial, une priorité nationale », rapport d'information présenté par M. Jean-Marie Bockel en juillet 2012 http://www.senat.fr/notice-rapport/2011/r11-681-notice.html*

- 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.

CRÉDITS DE L'ACTION 2 « COORDINATION DE LA SÉCURITÉ ET DE LA DÉFENSE » DU PROGRAMME 129 « COORDINATION DU TRAVAIL GOUVERNEMENTAL » DE LA MISSION « DIRECTION DE L'ACTION DU GOUVERNEMENT ».

	Titre 2	Hors titre 2	**Total**
Autorisations d'engagement	64 294 320	197 192 881	**261 487 201**
Crédits de paiement	64 294 320	229 007 863	**293 302 183**

Source : Projet annuel de performance, projet de loi de finances

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), OUTIL DE GESTION DES CRISES

Le SGDSN assure des missions relevant directement de la défense et de la sécurité, telles 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 la **cyberdéfense** ou encore la participation à l'élaboration de textes de doctrine et de textes normatifs en matière de défense et de sécurité nationale.

Plus précisément, l'action du Secrétariat général de la défense et de la sécurité nationale recouvre les missions suivantes :

- coordination interministérielle : il assure le secrétariat des conseils de défense et de sécurité nationale dans toutes ses formations, préside les instances et travaux interministériels relatifs à la politique de défense et de sécurité nationale et participe à l'analyse des crises internationales pouvant affecter notre environnement de sécurité ;

- planification de gestion de crise : il élabore la planification interministérielle de défense et de sécurité nationale et veille à sa mise en œuvre ;

- transmissions gouvernementales : il organise les moyens de commandement et de communication nécessaires au Gouvernement en matière de défense et de sécurité nationale et en fait assurer le fonctionnement ;

- sécurité des systèmes d'information : en qualité d'expert national, il propose et met en œuvre la politique du Gouvernement en la matière et apporte son concours aux services de l'Etat dans ce domaine ;

- coordination technologique : il veille à la cohérence des actions en matière de recherche et développement de projets technologiques intéressant la défense et la sécurité nationale et contrôle les exportations d'armement et les transferts de technologie sensible ;

- coordination des enseignements de défense et de sécurité comprenant la tutelle de l'Institut des hautes études de défense nationale (IHEDN) et de l'Institut national des hautes études de la sécurité et de la justice (INHESJ) ;

- coordination du renseignement : il apporte son appui à l'action du coordonnateur national du renseignement.

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

a) Le SGDSN assure le secrétariat des Conseils de défense, mène des travaux d'anticipation stratégique et assure le suivi des crises internationales

Outre le secrétariat des Conseils de défense et de sécurité nationale dans ses différents formats, le SGDSN assure le suivi des conflits et des crises internationales susceptibles d'affecter les intérêts français, en particulier ceux dans lesquels les forces armées sont engagées. Il anime des travaux interministériels d'analyse sur l'actualité internationale. En fonction de l'actualité, le SGDSN peut être ponctuellement sollicité pour produire des synthèses ou des recommandations sur l'évolution de la situation dans certains pays. **En 2013, six pays ont ainsi fait l'objet de travaux.**

Conformément au Livre blanc de 2013, le SGDSN anime un **comité interministériel de la prospective,** présidé par le Secrétaire général, visant à s'assurer de la cohérence et de la coordination des études de prospective menées par les différents ministères.

Le SGDSN suit les **questions d'ordre stratégique**, telles que le terrorisme, la défense anti-missiles balistiques (DAMB), la sécurité transatlantique et européenne, le désarmement et la maîtrise des armements, la lutte contre les menaces liées aux flux illicites ou encore la lutte contre la piraterie maritime.

Son rôle est de coordonner la réflexion interministérielle afin de proposer au Président de la République et au Gouvernement des orientations et des moyens d'action permettant de renforcer la sécurité nationale. À cet effet, le SGDSN réalise une évaluation mensuelle de la **menace terroriste** et assure une coordination interministérielle sur la **DAMB**. En 2013, le SGDSN a contribué à la mise en place d'un groupe interministériel sur la **dissémination des armements conventionnels**, en vue de renforcer la lutte contre les trafics et d'aider les Etats d'Afrique francophone (en priorité) à mettre en place les outils de contrôle des armements prévus dans le cadre du Traité sur le commerce des armes.

Depuis plusieurs années, le SGDSN suit la mise en œuvre d'une « *Stratégie Sahel* », dont l'objectif est de renforcer les capacités de souveraineté et de gouvernance des pays de la zone sahélo-saharienne. Il a également été chargé d'un **mandat sur la « prévention de la radicalisation ».**

EXEMPLES D'ANALYSES DU RISQUE PAR LE SGDSN

Dans le domaine particulier des explosifs, le SGDSN finance depuis 2006 des travaux d'évaluation de la menace terroriste fondée sur les explosifs artisanaux et définit sur cette base les mesures de protection à mettre en œuvre et les technologies de détection à développer.

Dans le secteur du transport aérien, après la création le 1er janvier 2013 d'une cellule d'analyse de risque au sein de la *direction générale de l'aviation civile* (DGAC), le SGDSN a poursuivi, en lien avec les ministères concernés, la supervision des dispositifs permettant d'évaluer le risque pour les vols en provenance de pays jugés sensibles et de lutter contre la menace des missiles sol-air de courte portée (« MANPADS »).

Source : réponse du Gouvernement au questionnaire parlementaire de la commission

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

Le SGDSN mène des 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**.

Le SGDSN coordonne la réponse nationale aux **interceptions proliférantes** réalisées dans le cadre de la PSI (*Proliferation Security Initiative*). La fréquence de ces interceptions ne cesse de croître depuis sa mise en œuvre en 2003. Neuf affaires d'interception de biens proliférants ont ainsi été menées dans ce cadre depuis l'été 2013[1].

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), la loi prévoyant un dispositif d'inspection sur mise en demeure sur le sol français.

Dans le domaine **biologique**, le SGDSN assure notamment la coordination des travaux sur la biologie de synthèse, domaine en pleine expansion, et coordonne la coopération de la France avec les Etats-Unis portant sur les différents volets de la défense biologique.

Le régime des **autorisations d'exportation** des matériels de guerre a été réformé par le « paquet défense » et sa loi de transposition de 2011[2]. L'exportation de matériels de guerre hors de l'Union européenne est désormais soumise à l'obtention d'une **licence**, délivrée 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).

---

[1] *Source : réponse du Gouvernement au questionnaire de la commission.*

[2] *Voir les travaux de votre commission sur la loi n° 2011-702 du 22 juin 2011 qui transpose notamment la directive européenne 2009/43 du 6 mai 2009 sur les transferts intracommunautaires de produits liés à la défense.*

Votre commission souligne que la modernisation, engagée depuis plusieurs années, des outils (notamment informatiques) de traitement des demandes, tendant à réduire les délais de traitement administratif (sans porter atteinte, naturellement, à la robustesse de l'instruction en elle-même), semble avoir désormais débouché : après une période de transition, le nouveau système de traitement « SIGALE » est en place.

Le SGDSN a également coordonné les travaux d'adoption de trois nouveaux arrêtés relatifs à la mise en place des « licences générales », notamment au bénéfice des forces armées françaises situées hors du territoire national. **Votre commission, qui avait soutenu cette mesure de simplification lors de l'examen de la loi de 2011, se félicite de la mise en œuvre de la loi.**

BILAN DE LA CIEEMG (2013-1er semestre 2014)

Au cours de l'année 2013 et du premier semestre 2014, la CIEEMG s'est réunie 17 fois en session plénière. En 18 mois, la CIEEMG a examiné 6 069 dossiers de demandes d'autorisation déposés par les entreprises, soit :

4 120 dossiers examinés en CIEEMG, sur lesquels 173 avis défavorables ont été rendus :

Année	Dossiers examinés en CIEEMG	Avis favorables[1]	Avis défavorables
2013	2 824	2 700	124
1er semestre 2014 (jusqu'au 31 mai)	1 296	1 247	49

Source : réponse du gouvernement au questionnaire de votre commission

2. Le SGDSN acteur de 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

Engagée fin 2012, la révision en profondeur du plan VIGIPIRATE s'est achevée en février 2014. Le nouveau plan se veut plus efficace par une meilleure adéquation des stratégies de protection et des mesures prises, par une communication au public d'une grande partie du plan, par une information sur la menace terroriste et sur les mesures engagées, et par une simplification des niveaux d'alerte.

[1] *Outre les avis favorables ou défavorables, la CIEEMG peut également proposer d'ajourner des dossiers.*

Le SGDSN achève actuellement la révision du plan « PIRATAIR-INTRUSAIR » qui vise à répondre à des actes illicites mettant en jeu la sûreté aérienne ou la souveraineté aérienne. Le SGDSN engagera par la suite la rénovation du plan « PIRANET » (réponse à des attaques sur les systèmes d'information).

À la suite de la catastrophe de FUKUSHIMA, un nouveau « *Plan national de réponse à un accident nucléaire ou radiologique majeur* » a été élaboré sous l'égide du SGDSN, qui a été rendu public en février 2014. Il fixe l'organisation de la gestion de crise, les stratégies à appliquer et les principales mesures à prendre au niveau gouvernemental. La déclinaison de ce plan au niveau des zones de défense et de sécurité et des départements sera effectuée en 2015, sous le pilotage du ministère de l'intérieur.

b) La consolidation des dispositifs interministériels de prévention et de protection : l'exemple des centrales nucléaires et du plan Ebola

S'agissant de la protection physique des **installations nucléaires**, le SGDSN a conduit des travaux qui ont donné compétence aux préfets de département pour réglementer la circulation et le stationnement aux abords des installations nucléaires. Les travaux se poursuivent sur le statut juridique des emprises des installations nucléaires, ainsi que sur les capacités des services internes de sécurité et les dispositifs de protection physique des opérateurs nucléaires.

L'audition du Secrétaire général par votre commission a mis en valeur le rôle du SGDSN dans l'élaboration, à la fois juridique et capacitaire, de la réponse s'agissant des récents survols de centrales par des drones.

De la même façon, le SGDSN a été la cheville ouvrière du récent « Plan Ebola » publié le 24 novembre dernier.

Le plan national de protection et de lutte contre Ebola

Le plan national de protection et de lutte contre Ébola a été publié le 24 novembre 2014. Ce document élaboré par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) à la demande du président de la République et du Premier ministre, a été adressé aux préfets et aux directeurs des Agences régionales de santé (ARS).

Il vise à préparer notre pays à tous les scénarios possibles, en graduant les réponses pour rester au plus près de la réalité épidémique et en définissant une stratégie générale de prévention et de lutte (incluant les domaines sanitaire, la protection du territoire, la continuité de l'activité économique, la recherche et le développement...).

Ce plan interministériel se veut ciblé, réactif et adaptable. Les mesures déjà prises (en matière de santé et de contrôles aux aéroports notamment, par exemple) correspondant à la réalité épidémique à la date de publication du plan.

Il s'agit d'un outil d'aide à la décision pour les responsables gouvernementaux, les représentants de l'État au niveau territorial et à l'étranger. Ce plan s'adresse également aux élus des collectivités locales, aux professionnels de santé et assimilés, ainsi qu'aux décideurs de nombreux domaines de la vie publique.

Source : Dépêches de presse et site du SGDSN

c) L'amélioration de l'organisation gouvernementale de réponse aux crises majeures : le « Contrat général interministériel »

L'Etat doit organiser et mettre en œuvre des capacités civiles et militaires pour faire face aux multiples risques et menaces qui peuvent affecter le pays. Si la planification capacitaire existe de longue date pour ce qui concerne l'engagement des armées, au travers des « contrats opérationnels » qui leurs sont fixés, cette démarche faisait défaut dans le champ des **ministères civils** qui doivent intervenir les premiers face aux risques et aux menaces non armées.

Le *contrat général interministériel* répond à cette exigence en fixant, pour les 5 années à venir (2015-2019), les **capacités critiques des ministères civils et le niveau d'engagement** de ceux-ci dans la réponse aux crises majeures. Ces capacités sont fixées dans un cadre de juste suffisance et de complémentarité avec les autres acteurs de la gestion des crises que sont les armées, les collectivités territoriales et les opérateurs d'importance vitale.

À l'issue d'un travail interministériel mené en 2013 sous l'égide du SGDSN, le « Contrat général interministériel » a été approuvé par le cabinet du Premier ministre en mai 2014. Pour les outre-mer, ces capacités seront complétées par l'élaboration d'un programme quinquennal d'équipements mutualisés.

D'après les réponses fournies par le Gouvernement au questionnaire écrit de vos rapporteurs, **la déclinaison territoriale de cette démarche capacitaire sera effectuée d'ici 2016**, sous la responsabilité du ministère de l'Intérieur.

S'agissant de la capacité de **veille et d'alerte** sur les différentes crises au profit des hautes autorités de l'Etat, Le SGDSN est un acteur essentiel de la chaîne d'alerte gouvernementale, dispositif qui s'appuie notamment sur le *Bureau de veille et d'alerte* (BVA) du SGDSN, qui coordonne étroitement ses actions avec les centres opérationnels des ministères, vingt-quatre heures sur vingt-quatre. Son efficacité est cruciale, notamment pour la gestion éventuelle d'une épidémie comme celle de fièvre *Ebola* ou encore en cas d'accident aérien impliquant des ressortissants français.

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

Le SGDSN est partie prenante du renforcement du fonctionnement de la ***cellule interministérielle de crise*** (CIC) qui est au cœur du dispositif

gouvernemental de gestion des crises majeures. La démarche de professionnalisation des acteurs de la gestion de crise, engagée en 2012, s'est poursuivie avec notamment l'élaboration en 2014 d'un *référentiel interministériel de formation*, première étape de la création au sein des administrations d'un véritable « réservoir de compétences » spécialisé dans la gestion de crise.

S'agissant des **exercices gouvernementaux**, après une année 2013 consacrée aux risques naturels et technologiques, l'année 2014 a été dédiée à la **thématique terroriste**. Outre l'évaluation des plans VIGIPIRATE et PIRATAIR rénovés en 2014, le renforcement de la coordination politico-stratégique entre la France et le Royaume-Uni en cas de crise majeure a été poursuivi. L'organisation d'un exercice de grande ampleur simulant une crue majeure de la Seine, à l'initiative de la Préfecture de Police, est envisagée pour tester le plan relatif à la continuité du travail gouvernemental et les plans ministériels de continuité d'activité.

e) La consolidation d'une filière industrielle française de sécurité informatique

Votre commission avait mis en lumière, dans son rapport d'information précité de juillet 2012, la nécessité de consolider une filière industrielle française de la sécurité informatique.

Priorité n° 7 du rapport d'information de 2012 sur la cyberdéfense : Soutenir par une politique industrielle volontariste, à l'échelle nationale et européenne, le tissu des entreprises françaises, notamment des PME, spécialisées dans la conception de certains produits ou services importants pour la sécurité informatique et, plus largement, du secteur des technologies de l'information et de la communication, et renforcer la coopération entre l'Etat et le secteur privé.

Pour répondre au besoin de sécurité informatique de l'Etat et des *opérateurs d'importance vitale* (OIV) et conformément à ces recommandations, le SGDSN a initié et conduit les travaux interministériels visant à structurer les industries françaises dans le domaine de la sécurité informatique. Le Premier ministre a ainsi installé, le 23 octobre 2013, le *Comité de la filière industrielle de sécurité* (CoFIS) rassemblant onze ministres, des représentants des collectivités territoriales et du Parlement, des dirigeants de sociétés qui développent ou utilisent des solutions de sécurité, des présidents de pôles de compétitivité ainsi que des membres éminents de la recherche académique française. Le CoFIS est destiné à promouvoir la compétitivité de la filière, en cohérence avec les 34 plans de la « Nouvelle France industrielle » et la stratégie nationale de recherche. Il porte sur un secteur sensible qui participe à notre autonomie stratégique.

D'après les réponses écrites transmises par le Gouvernement au questionnaire écrit de votre commission, **pour 2014 et 2015,** l'objectif principal sera d'accompagner la montée en puissance du dispositif, de lancer

les premiers démonstrateurs technologiques de la filière et de poursuivre une politique de financement de la recherche et de l'innovation dans le domaine de la sécurité.

Le Gouvernement indique ainsi dans ses réponses écrites que le SGDSN « *continuera à participer au financement de l'Agence nationale de la recherche et du Fonds unique interministériel, tout en finançant en propre le développement de nouvelles solutions de lutte contre les menaces nucléaires, radiologiques, biologiques, chimiques et liées aux explosifs. Il poursuivra, par ailleurs, son action de promotion des intérêts français auprès de la Commission européenne dans le cadre du programme européen « Horizon 2020* » ».

3. Les moyens du SGDSN dans le projet de loi de finances pour 2015

Le budget du SGDSN dans le projet de loi de finances pour 2015 s'élève à **211,3 millions d'euros** en autorisations d'engagements et **243,1 millions d'euros** en crédits de paiement.

CRÉDITS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2015

(EN MILLIONS D'€)

	LFI 2014		**PLF 2015**	
	AE	CP	AE	CP
Titre 2	47,66	47,66	64,29	64,29
dont transfert CTG[1]			12,88	12,88
HT2	144,47	146,52	146,99	178,81
TOTAL	192,12	194,17	**211,29**	**243,10**

La hausse du budget du SGDSN reflète la montée en puissance de la politique de sécurité des systèmes d'information, qui se concrétise par une hausse des crédits et emplois de l'ANSSI depuis 2009 (cf. ci-dessous). Le plafond d'emplois du SGDSN (hors ANSSI) relève quant à lui des orientations du Premier ministre pour les secteurs non prioritaires, et se traduit donc par une **diminution de 3 emplois sur la période 2015-2017** (-1 ETP chaque année).

[1] *Transfert du Centre de transmission du Gouvernement.*

RÉALISATION DES EMPLOIS DU SGDSN

Catégorie d'emplois	**Plafond LFI 2014** (en ETPT)	**Effectifs SGDSN au 30 juin 2014** (en ETP)	**dont ANSSI** (en ETP)
Catégorie A+	79	56	30
Catégorie A	84	68	32
Catégorie B	48	35	14
Catégorie C	86	92	24
Contractuels	298	319	261
TOTAL	**595**	**570**	**361**

De même, l'évolution du budget (hors ANSSI) applique les orientations générales du Gouvernement du budget triennal 2015-2017, soit une diminution globale de 5% des crédits à échéance de 2015 - et de 15% à échéance de 2017 - par rapport à la loi de finances pour 2014.

B. L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI), BRAS ARMÉ DE L'ETAT POUR LA CYBERDÉFENSE

1. La cyberdéfense désormais élevée au rang de priorité nationale

a) Un risque croissant désormais reconnu comme une priorité

Votre commission avait estimé dans son rapport de 2012 qu'il convenait d'élever la cyberdéfense au rang d'une véritable priorité nationale.

Priorité n° 1 du rapport d'information « cyber » de 2012 : Faire de la cyberdéfense et de la protection des systèmes d'information une priorité nationale, portée au plus haut niveau de l'Etat, notamment dans le contexte du nouveau Livre blanc.

De fait, l'étendue de la menace ne cesse de s'accroître. La France est classée au 15ème rang mondial des pays où la cybercriminalité est la plus active[1].

[1] *Rapport de la société américaine de sécurité informatique Symantec.*

L'augmentation exponentielle des cyberattaques

D'après le dernier rapport de la société américaine de sécurité informatique Symantec[1], les cyberattaques ont augmenté de 91% en 2013. En France, les PME seraient les plus visées, en tant que porte d'entrée vers les plus grands groupes : les attaques ciblées viseraient à 77% des PME et organisations de moins de 250 salariés.

La durée des attaques aurait également significativement augmenté. Les attaques seraient de plus en plus ciblées, passant d'attaques envoyées sur des dizaines de milliers d'ordinateurs à des attaques choisies en fonction de la cible très précisément recherchée. Les assistants personnels et les spécialistes des relations publiques seraient des cibles privilégiées, comme moyen d'accéder aux chefs d'entreprises ou à des personnes en responsabilité.

Coordonnées bancaires, données commerciales, propriété industrielle, informations gouvernementales, sont des cibles prioritaires. Le nombre de violations de données aurait augmenté de 62% entre 2012 et 2013, avec au total 552 millions d'identités qui auraient été utilisées.

Huit attaques de très grande ampleur auraient été recensées en 2013 (contre une seule de cette nature en 2012).

Après les mobiles et les tablettes, les attaques via les objets connectés seraient une cible croissante des cyberattaques.

Source : Symantec

Encore tout récemment, des sites de média ont récemment été la cible d'attaques informatiques : les sites de *France Inter* et de *France Info* ont été rendus inaccessibles, jeudi 9 octobre 2014, vraisemblablement suite à une attaque informatique par déni de service (saturation d'un site par « fausses » requêtes pour en bloquer l'accès).

Outre un accroissement quantitatif, on observe en outre un accroissement qualitatif des attaques et surtout un accroissement de leur champ, qui se déplace du terrain de l'Internet et de la bureautique vers celui des applications industrielles, soit à des fins d'espionnage, soit pour perturber le fonctionnement des services.

Le **nouveau Livre blanc** sur la défense et la sécurité nationale, publié en avril 2013, a marqué une nouvelle et importante 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 »*.

[1] *Source : dépêche de l'AFP sur le rapport annuel de Symantec, 8 avril 2014.*

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'Etat, 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'Etat 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.

Ces orientations ont été mises en œuvre dans la loi de programmation militaire du 18 décembre 2013, puis déclinées par l'adoption d'un « *pacte défense cyber* ». Ce pacte, présenté en février 2014, comporte cinq axes (cf. ci-après) et fait intervenir tant le ministère de la défense (officier général « *cyberdéfense* » et sa chaîne opérationnelle, DGA, DGSE) que le ministère de l'intérieur (DGSI, DGGN, centre opérationnel de sécurité de Toulouse) et, au premier chef, l'ANSSI, autorité nationale en matière de sécurité et de défense des systèmes d'information.

b) Un cadre législatif et réglementaire renforcé

Priorité n° 3 du rapport de 2012 : Introduire des modifications législatives pour donner les moyens à l'ANSSI d'exercer ses missions (...) ;

Priorité n° 5 du rapport de 2012 : Rendre obligatoire pour les entreprises et les opérateurs d'importance vitale une déclaration d'incident à l'ANSSI en cas d'attaque importante contre les systèmes d'information et encourager les mesures de protection par des mesures incitatives.

(1) Des dispositions législatives figurant au sein de la loi de programmation militaire du 18 décembre 2013

Le chapitre IV de la loi relative à la programmation militaire pour les années 2014 à 2019 contient des « *Dispositions relatives à la protection des infrastructures vitales contre la cybermenace* ».

Trois principales dispositions ont été adoptées, avec le soutien ou à l'initiative de votre commission.

L'article 21 (Articles L. 2321-1 et L. 2321-2 nouveaux du code de la défense) vise le renforcement du dispositif étatique en matière de cyberdéfense. Il tend, en premier lieu, à consacrer au niveau législatif la **compétence du Premier ministre** en matière de protection et de défense des systèmes d'information. En deuxième lieu, il reconnaît la possibilité pour les services compétents de l'Etat, en cas d'attaque informatique importante visant les intérêts fondamentaux de la Nation, d'accéder aux systèmes d'information qui sont à l'origine de l'attaque. En dernier lieu, il permet aux services de l'Etat déterminés par le Premier ministre de détenir des équipements ou des programmes informatiques susceptibles d'être utilisés lors d'attaques informatiques (comme des virus informatiques par exemple) afin d'analyser leur conception et d'observer leur fonctionnement.

L'article 22 (Articles L. 1332-6-1 à L. 1332-6-6 nouveaux du code de la défense et article L. 1332-7 du code de la défense) tend au renforcement des **obligations des opérateurs d'importance vitale** en matière de sécurité et de défense des systèmes d'information. Il prévoit notamment l'obligation de notifier les incidents informatiques importants ou la réalisation d'audits réguliers.

Il s'agit d'un changement majeur : jusqu'alors, l'ANSSI avait un rôle essentiellement de conseil et d'alerte. C'est sur ce fondement qu'elle a naturellement, depuis plusieurs années, assis la sensibilisation des acteurs économiques, par exemple autour des risques liés au développement du *cloud computing*. Désormais, elle dispose de pouvoirs d'action étendus.

L'article 24 (Article L. 2321-3 nouveau du code de la défense, articles L.336-3 et L. 34-1 du code des postes et des communications électroniques) prévoit un **accès aux coordonnées des utilisateurs des adresses Internet** pour les besoins de la sécurité informatique.

Cet article, **introduit dans la loi à l'initiative du Sénat**, vise à permettre aux agents de l'Agence nationale de la sécurité des systèmes d'information, habilités par le Premier ministre et assermentés dans des conditions fixées par décret en Conseil d'Etat, d'obtenir des opérateurs de communications électroniques l'identité, l'adresse postale et l'adresse électronique d'utilisateurs ou de détenteurs de systèmes d'information vulnérables, menacés ou attaqués.

(2) Une entrée en vigueur toujours conditionnée à la parution des textes d'application

L'entrée en vigueur de certaines dispositions de la loi est conditionnée à la parution de décrets d'application. **Votre commission insiste sur la nécessité de mener rapidement ce chantier réglementaire à terme pour donner aux dispositions législatives leur plein effet.**

Pour la mise en application de l'alinéa 2 de l'art. L. 2321-2 du code de la défense (créé par l'article 21 de la loi de programmation) qui légalise la détention et l'analyse de codes malveillants pour les services de l'Etat désignés par le Premier ministre, l'ANSSI mène une concertation interministérielle destinée à définir une liste restreinte des services de l'Etat qui seront autorisés à bénéficier de cette disposition**. Un arrêté du Premier ministre devrait rendre publique cette liste[1].**

Un **décret en Conseil d'Etat** doit notamment venir préciser les obligations qui pèsent sur les opérateurs d'importance vitale.

Pour la mise en œuvre des dispositions précitées donnant au Premier ministre les capacités nouvelles pour protéger les opérateurs d'importance vitale (alinéas 1 à 6 de l'article L. 1332-6 du code de la défense, introduit par l'article 22 de la loi de programmation militaire), l'ANSSI a engagé un travail de concertation et de préparation dès 2013. Des expériences pilotes ont été menées en étroite collaboration avec certains opérateurs volontaires, notamment en ce qui concerne l'identification et la définition de la criticité de leurs systèmes d'informations ou les processus de notification des incidents.

D'après les informations communiquées à votre commission, le projet de décret d'application fait l'objet d'une concertation interministérielle. Il sera ensuite transmis au Conseil d'Etat.

Parallèlement, un travail par secteur d'importance vitale est engagé, sous l'égide de l'ANSSI, afin de prendre en compte la spécificité de chaque secteur, voire de chaque sous-secteur et, dans certains cas, de l'opérateur. Les ministères de tutelle des opérateurs, les autorités de contrôles du secteur d'activité d'importance vitale lorsqu'elles existent, et les opérateurs eux-mêmes sont associés à ces travaux.

Comme l'a confirmé lors de son audition le directeur de l'ANSSI, les arrêtés sectoriels (publics ou classifiés) préciseront les obligations des opérateurs. Ils seront publiés, pour l'essentiel, courant 2015.

Les premiers groupes de travail dédiés à la préparation de ces règles de sécurité ont été **lancés mi-octobre 2014 pour les secteurs de l'énergie (électricité et gaz) et des communications électroniques[2]**.

Mis en place d'ici le début d'année 2015 pour chaque domaine d'activité (eau, énergie, finances, transports, etc.), ces groupes rassemblent, autour de l'ANSSI, les opérateurs d'importance vitale, les ministères coordonnateurs et les autorités sectorielles.

L'objectif de ce travail collectif est de définir les systèmes d'information concernés et des règles efficaces, soutenables et adaptées aux

---

[1] *Source : réponse du Gouvernement au questionnaire de votre commission.*

[2] *Source : http://www.ssi.gouv.fr/fr/menu/actualites/cybersecurite-et-loi-de-programmation-militaire-preparation-des-regles-de.html*

métiers et spécificités des opérateurs, et de garantir la bonne articulation de ce nouveau dispositif avec les réglementations préexistantes.

La disposition introduite par le Sénat à l'article L. 2321-3 du code de la défense et qui donne aux agents de l'ANSSI la possibilité d'obtenir de la part des opérateurs de communications électroniques les **coordonnées de victimes d'attaques informatiques** doit elle aussi être précisée par décret pour définir les conditions d'habilitation et d'assermentation par le Premier ministre des agents de l'ANSSI autorisés à utiliser cette disposition. Le décret a été transmis au Conseil d'Etat, après avis de la Commission nationale informatique et libertés (CNIL).

(3) Une sensibilisation de l'ensemble du Gouvernement par circulaire du Premier ministre : la « PSSIE »

Le Premier ministre a publié en juillet 2014 une circulaire à destination de tous les ministres et secrétaires d'Etat, fixant les règles de protection des systèmes d'information des différents départements ministériels. Ce document de 40 pages, préparé par l'ANSSI, qui fixe les contours d'une « *Politique de sécurité des systèmes d'information de l'Etat* » (PSSIE) est un instrument de diffusion des bonnes pratiques dans l'ensemble des ministères.

Elle décline dix principes fondamentaux portant sur le choix d'éléments de confiance pour construire les systèmes d'information, sur la gouvernance de la sécurité et sur la sensibilisation des acteurs. Les administrations sont désormais tenues de recourir à des produits et services qualifiés par l'ANSSI et d'héberger leurs données sensibles sur le territoire national.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Paris, le 17 juillet 2014
N° 5725/SG

Le Premier Ministre

à

Mesdames et Messieurs les ministres
Mesdames et Messieurs les secrétaires d'Etat

Objet : Politique de sécurité des systèmes d'information de l'Etat
Annexe : Document de politique de sécurité des systèmes d'information de l'Etat

Les systèmes d'information sont devenus indispensables à l'efficacité de l'action publique. Ils contribuent de manière structurante à la plupart des missions essentielles des ministères.

L'ouverture croissante des systèmes d'information et leur interconnexion engendrent de nouvelles vulnérabilités. Les menaces d'exfiltration de données confidentielles, d'atteinte à la vie privée des usagers, voire de sabotage des systèmes d'information se multiplient. Afin d'y répondre, le Gouvernement met en œuvre par la présente circulaire une politique de sécurité des systèmes d'information de l'Etat.

Le document annexé fixe un ensemble de règles de protection applicables aux systèmes d'information de l'Etat. Ces règles ont été élaborées par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), en liaison avec les ministères. Elle prennent en compte les constats effectués par l'agence lors de ses inspections et lors de traitements d'incidents.

En préambule, sont énoncés des principes de sécurité incontournables, notamment l'obligation d'acquérir des produits et des services de sécurité labellisés par l'ANSSI et l'hébergement des données sensibles sur le territoire national.

Je vous demande d'appliquer la présente politique de sécurité des systèmes d'information de l'Etat aux systèmes d'information de votre ministère.

La sécurité informatique de l'Etat dépend de l'efficacité de la mise en œuvre des règles énoncées. Je souhaite que ce dossier soit suivi avec toute l'attention nécessaire. L'ANSSI se tient à la disposition de vos services pour les accompagner dans l'application de cette politique.

Manuel VALLS

Il faut relever que, ministère de la défense mis à part, le niveau de prise de conscience et de réponse apportée, notamment en moyens, face aux cyberattaques, est très variable suivant les ministères. L'enjeu est désormais de diffuser cette culture au-delà de la seule sphère « sécurité-défense ».

c) La mobilisation du ministère de la défense sur l'enjeu « cyber »

(1) La mise en œuvre du « *Pacte défense cyber* »

Même s'il n'est pas le seul concerné, le ministère de la défense a une exigence particulière en matière de cyberdéfense, ne serait-ce que parce qu'il met en œuvre les moyens de la dissuasion nucléaire et qu'il conduit les interventions militaires en opérant pour ce faire des systèmes d'information et de communications particulièrement complexes (notamment pour les systèmes d'armes sophistiqués : aéronefs de combat ou de transport, navires de surface ou sous-marins, véhicules de combat terrestres…).

Le ministère de la défense est naturellement particulièrement concerné par la menace cyber.

Lors de la présentation du « Pacte défense Cyber », le ministère de la défense a ainsi révélé[1] que *« les attaques significatives contre les systèmes du ministère ont approché les 800 en 2013, ce qui représente un doublement chaque année.* ».

Ce plan d'action est destiné à rassembler toutes les actions conduites en matière de cyberdéfense par le ministère de la défense jusqu'en 2016. Son exécution est suivie au travers d'indicateurs précis. Il a vocation à rassembler au-delà du seul ministère de la défense, les industriels et PME/PMI, les organismes de recherche, mais aussi les organismes de formation.

Au total, le ministère de la défense indique qu'un milliard d'euros seront investis pour la cybersécurité d'ici 2019.

Les 6 priorités du « pacte défense Cyber »

Axe 1 : Durcir le niveau de sécurité des systèmes d'information et les moyens de défense et d'intervention du ministère et de ses grands partenaires de confiance.

Axe 2 : Préparer l'avenir en intensifiant l'effort de recherche tant technique et académique qu'opérationnel, tout en soutenant la base industrielle.

Axe 3 : Renforcer les ressources humaines dédiées à la cyberdéfense et construire les parcours professionnels associés.

Axe 4 : Développer le Pôle d'excellence en cyberdéfense en Bretagne au profit du ministère de la défense et de la communauté nationale de cyberdéfense.

Axe 5 : Cultiver un réseau de partenaires étrangers, tant en Europe qu'au sein de l'Alliance atlantique et dans les zones d'intérêt stratégique.

Axe 6 : Favoriser l'émergence d'une communauté nationale défense de cyberdéfense en s'appuyant sur un cercle de partenaires et les réseaux de la réserve.

Source : DICOD

[1] *Source : pacte défense cyber, DICOD*

(2) L'exercice « *Defnet 2014* »

Exercice interarmées DEFNET 2014

Du 30 septembre au 3 octobre 2014 s'est déroulé l'exercice interarmées de cyberdéfense DEFNET 2014 sur le site des écoles de Saint-Cyr Coëtquidan regroupant une soixantaine d'experts de la cyberdéfense.

Novateur, cet exercice a consisté à simuler des réseaux civils et des réseaux militaires dans lesquels seraient injectés des logiciels malveillants, et à déployer simultanément en réponse trois groupes d'intervention rapide cyber et à activer une cellule de crise.

« DEFNET 2014 », véritable exercice de mise en situation, a permis de valider des procédures opérationnelles dans l'emploi de ces groupes d'intervention rapide. Il a aussi permis d'apporter des évolutions dans le format actuel de la formation et de l'instruction cyber. Joueurs, animateurs et observateurs provenant des armées, de plusieurs organismes du ministère de la défense et d'entreprise partenaires, ont œuvré ensemble durant 4 jours, contribuant ainsi à renforcer les liens au sein de la communauté de cyberdéfense. Les différentes entités au sein de l'exercice ont pu progresser dans leur domaine respectif :

. La cellule de crise s'est entraînée au partage de l'information et à la conduite des actions défensives de cyberdéfense au profit d'un déploiement opérationnel et d'une entreprise de défense.

. Les membres des trois GIR (Terre, Air, DIRISI/Marine) ont développé leur capacité à intervenir ensemble dans un environnement complexe en vue de renforcer les capacités permanentes d'intervention.

Le développement d'une plate-forme avec les entreprises privées partenaires a permis de simuler des environnements complexes et de mener des investigations techniques en profondeur dans les réseaux. Cela a ainsi augmenté le réalisme de l'instruction. Une étape clé a ainsi été franchie lors de cet exercice riche d'enseignements qui pourrait également être répliqué au sein des grandes entreprises stratégiques ou être exporté auprès de pays alliés.

Source : ministère de la défense

L'intérêt de cette « manœuvre » militaire d'un nouveau type est à souligner, tant elle constitue une occasion de **renforcer la chaîne de cyberdéfense au sein du ministère de la défense.**

« DEFNET 2015 », prochaine édition de cet entraînement interarmées, est prévu en mars 2015.

d) La mise en place d'un réseau unifié et sécurisé : le réseau interministériel de l'Etat (RIE)

Les administrations de l'Etat sont des cibles potentielles pour les attaques informatiques, comme l'ont montré les attaques sur le réseau du ministère de l'économie et des finances, les suspicions d'attaques sur celui de l'Élysée ou celles sur le site Internet du Sénat par exemple.

Dès 2011, l'Etat a donc mis en chantier un réseau informatique unifié et sécurisé, destiné tout à la fois à mieux maîtriser la sécurité dans un

contexte de cyberattaques croissantes, mais aussi à améliorer le service rendu aux citoyens en facilitant les échanges entre les administrations et le développement d'applications partagées. Ce projet**, à la fois de sécurité et de modernisation de l'Etat**, est porté par les services du Premier ministre (la DISIC, direction interministérielle de l'information et de la communication[1]).

Le décret n° 2014-879 du 1er août 2014 relatif au système d'information et de communication de l'Etat est venu affirmer cette « unicité » du système d'information de l'Etat.

Sans tendre à l'uniformité, ce qui serait trop complexe, le but est de faire partager une même vision aux ministères et de privilégier des choix technologiques communs, afin d'imprimer une cohérence globale en raccordant l'ensemble des sites ministériels, des administrations centrales et déconcentrées, pour faciliter les échanges interministériels, dans un système sécurisé.

Ce projet de grande ampleur, puisque 17 000 sites seront progressivement reliés entre 2013 et 2017, avait un coût de construction initial évalué à 11,5 millions d'euros, pour un coût de fonctionnement annuel de 6,5 millions d'euros[2]. Ce réseau est destiné à remplacer progressivement l'ensemble des réseaux ministériels.

Le « cœur de réseau » à haut débit, qui relie douze centres informatiques ministériels, est déjà opérationnel, depuis l'été 2013.

Aujourd'hui il est déployé sur plus de 1 500 sites sur l'ensemble du territoire national et relie les ministères de l'agriculture, de l'écologie, de la santé, de l'intérieur, des finances, de la culture, du travail et les services du Premier ministre. Le déploiement sur 8 500 sites ministériels est d'ores et déjà engagé.

2. L'ANSSI : une action amplifiée, des moyens accrus

a) Des missions consolidées

C'est 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, qui a conduit à la création de l'ANSSI en 2009.

Votre commission avait d'ailleurs dès cette époque contribué à la prise de conscience de ce phénomène, avec des rapports d'information précurseurs pour alerter sur cette nouvelle menace.

L'ANSSI a la responsabilité de conduire ou de coordonner l'ensemble des actions destinées à prévenir les attaques contre les systèmes

---

[1] Créée par le décret n°2011-193 du 21 février 2011, la DISIC est placée sous l'autorité du Premier ministre et rattachée au Secrétariat général pour la modernisation publique.

[2] Hors coûts de raccordement des sites ministériels.

d'information, et à réagir en cas d'atteinte à leur confidentialité, à leur disponibilité ou à leur intégrité.

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'Etat s'est **élargi**, comme cela vient d'être dit, avec la loi de programmation militaire du 18 décembre 2013, aux opérateurs d'importance vitale, aux entreprises indispensables à la stratégie de sécurité nationale, et plus généralement, vers l'ensemble des acteurs de la société de l'information. Le Premier ministre peut dorénavant imposer des règles de sécurité informatique à ces opérateurs d'importance vitale, qui sont désormais tenus de déclarer les incidents majeurs intervenant sur leurs systèmes d'information.

La loi de programmation a également ouvert à l'ANSSI la possibilité de **détenir des codes malveillants** afin d'en observer le fonctionnement et l'évolution. Comme d'autres services de l'Etat désignés par le Premier ministre, en cas d'attaque informatique majeure, l'agence est désormais autorisée à **accéder aux systèmes d'information** à l'origine de l'attaque afin d'en faire cesser les effets. Enfin, ses agents peuvent obtenir des opérateurs de communications électroniques les **coordonnées de victimes** d'attaques informatiques afin de les avertir et de les protéger.

Le Livre blanc et la loi de programmation militaire de 2013 ont également confirmé, dans un cadre budgétaire pourtant contraint, la **poursuite de la croissance des moyens** de l'ANSSI, indispensable pour relever des défis toujours croissants.

b) Une action amplifiée

(1) La protection de l'information de souveraineté

En 2013, pour protéger les **communications les plus importantes** ou les plus secrètes des autorités de l'Etat, l'ANSSI a déployé 500 téléphones sécurisés « TEOREM » supplémentaires sur le réseau téléphonique ordinaire et sur le réseau « RIMBAUD » (réseau résilient destiné aux communications de crise, capable de fonctionner même lorsque les réseaux commerciaux des opérateurs ne fonctionnent plus correctement).

Le réseau de **données interministériel confidentiel défense « ISIS »**, utilisé pour coordonner la gestion de crises et pour l'échange de données très sensibles entre administrations, poursuit sa modernisation. En complément des offres résilientes conçues avec un opérateur privé, le service ISIS a été également ouvert sur le « Réseau cœur gouvernemental » (RCG) opéré à Paris par le Centre de transmissions gouvernemental (CTG) sur un ensemble de boucles optiques spécifiques. **Au total, 230 sites sont raccordés à ISIS, dont les deux tiers hors de l'Ile-de-France. On comptabilise 2 300 abonnés, sur 900 postes, qui ont échangé près de 500 000 courriers électroniques.**

Votre commission s'interroge d'ailleurs sur l'opportunité qu'il y aurait à connecter les deux assemblées du Parlement à ce réseau, pour améliorer la fiabilité des transmissions avec le Gouvernement.

LE CENTRE DE TRANSMISSIONS GOUVERNEMENTAL

Organisme militaire mis pour emploi auprès de l'ANSSI, le **centre de transmissions gouvernemental (**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. Il intervient dans la mise à disposition d'une partie des systèmes de télécommunications sécurisés nécessaires à la continuité de l'action de l'Etat.

(2) La détection des attaques informatiques

L'ANSSI développe depuis 2010 une capacité centralisée de **détection des attaques informatiques** visant les systèmes d'information des services de l'Etat. En 2013, des travaux d'amélioration du positionnement technique des systèmes de détection déjà en exploitation ont permis d'accroître de près de 25% le taux de couverture.

En parallèle, le centre de détection des attaques informatiques de l'ANSSI a industrialisé les solutions développées et amélioré ses capacités afin d'anticiper de nouvelles menaces. Les développements ont principalement porté, d'une part, sur l'intégration de nouvelles techniques de détection innovantes et, d'autre part, sur la conception de sondes haut-débit destinées à la supervision du Réseau interministériel de l'Etat (RIE).

Sur **plus de 1 600 « tickets d'incidents » concernant les systèmes d'information de l'Etat surveillés**, près de **340 ont donné lieu à des alertes**. L'agence a effectué 10 restitutions auprès des ministères afin d'apporter des préconisations indispensables à la bonne compréhension des attaques qui ont été détectées.

L'accroissement de l'activité opérationnelle de l'ANSSI et le besoin d'améliorer la coordination et le pilotage des opérations ont conduit à mettre en place une structure de centralisation et de pilotage des opérations de cyberdéfense, baptisé « **centre de cyberdéfense** », co-localisé avec le centre d'analyse de lutte informatique défensive (CALID) du ministère de la défense. En cas de crise, le dispositif opérationnel peut monter en puissance et le centre de cyberdéfense est capable d'accueillir entre 50 à 80 personnes.

L'ANSSI a une nouvelle fois constaté **une multiplication des attaques « critiques »,** conséquence à la fois de l'augmentation du nombre et de la virulence des attaques et du déploiement plus large de solutions de détection qui contribue mécaniquement à révéler de plus nombreux cas de compromissions.

(3) Le développement de la sécurité informatique pour l'ensemble de la société

L'ANSSI a publié dans ces douze derniers mois **16 guides et notes techniques** dans le cadre de sa mission de sensibilisation auprès des administrations, des acteurs économiques et du grand public. En outre, 6 articles scientifiques ont été publiés par les agents de l'ANSSI et 38 conférences scientifiques ou techniques ont été prononcées dans des manifestations spécialisées.

Dans le cadre de sa mission de soutien au développement d'une meilleure sécurité informatique pour l'ensemble de la société, l'ANSSI attribue un **label** attestant de la sécurité des produits qui lui sont soumis. Treize produits ont ainsi été qualifiés par l'ANSSI en 2013. Cinq produits ont été agréés pour la protection du niveau « Diffusion Restreinte » (national ou interallié) et deux pour la protection des informations classifiés « Confidentiel Défense » ou « Secret Défense ».

Dans le cadre de sa politique industrielle, l'ANSSI suit le positionnement de l'offre nationale de cybersécurité sur la scène internationale et identifie **les secteurs orphelins**. Elle établit une base de connaissance sur les entreprises du domaine et tient à jour un réseau de contacts appropriés au sein de la plupart des sociétés. La liste des entreprises suivies compte une proportion croissante de sociétés de services (30%). En une année, l'ANSSI a rencontré 270 industriels (75% de nationaux) pour des entretiens bilatéraux. Dans un cas sur deux, ce sont les sociétés elles-mêmes qui ont provoqué les rencontres. Le tiers d'entre elles ambitionne d'obtenir une labellisation de son offre par l'ANSSI.

L'ANSSI a participé, en liaison avec le commissariat général à l'investissement, la banque publique d'investissement (Bpifrance), la direction générale de l'armement (DGA) et la direction générale de la compétitivité, de l'industrie et des services (DGCIS), à l'élaboration de **l'appel à projet « sécurité numérique »** des investissements d'avenir, en identifiant notamment cinq axes de travail prioritaires.

Dans le même temps, **le « plan 33 »** parmi les 34 plans de « reconquête industrielle » du Gouvernement, **vise à fédérer et à mobiliser l'ensemble des acteurs publics et privés de la filière cybersécurité**, afin d'identifier et de mettre en œuvre tous les moyens propres à doter la France d'une **industrie de pointe dans ce secteur**. Son pilotage a été confié au directeur général de l'ANSSI. Les propositions ont été validées à l'été 2014.

Le centre de **formation** de l'ANSSI a reçu et formé 1 400 stagiaires durant l'année scolaire écoulée, soit un nombre équivalent à l'année précédente. Enfin, l'ANSSI a soutenu le ministère des affaires étrangères pour la sécurisation du vote électronique utilisé pour les élections législatives des Français établis hors de France.

(4) Audits

En 2013, les équipes de l'ANSSI ont mené **28 audits** au profit de la Présidence de la République, des services du Premier ministre, du ministère de la défense, du ministère des affaires étrangères, du ministère de la justice et du ministère de l'écologie, du développement durable et de l'énergie.

Dans le même temps, sept **inspections** ont été conduites. Elles ont porté sur les services du Premier ministre, les ministères économiques et financiers, le ministère des affaires sociales et de la santé, ainsi que le ministère du travail, de l'emploi, de la formation professionnelle et du dialogue social.

Enfin, des **contrôles** de sécurité au sens de l'article L33-10 du code des postes et communications électroniques ont été menés en 2013 à la demande du ministère en charge des communications électroniques

c) Une augmentation des moyens

Priorité n° 2 du rapport d'information de 2012 : Renforcer les effectifs, les moyens et les prérogatives de l'Agence nationale de sécurité des systèmes d'information, ainsi que les effectifs et les moyens dédiés au sein des armées, de la direction générale de l'armement et des services spécialisés, et développer une véritable politique des ressources humaines.

Au total, alors que l'Agence comptait à sa création en 2009 100 personnes, ses personnels sont aujourd'hui de l'ordre de 400, pour une montée en puissance programmée jusqu'à 600 effectifs fin 2017. Cela représente environ 50 embauches nettes par an.

Plus précisément, la programmation des finances publiques 2015-2017 prévoit que les **créations d'emplois** à l'ANSSI se poursuivront sur la période triennale. Le schéma d'emploi de l'ANSSI est ainsi fixé à **+145 équivalents temps plein,** dont **65 créations d'emplois dès 2015**, soit une nouvelle cible d'effectif de 487 agents en 2016 et **567 agents fin 2017**.

Pour autant, cette situation « privilégiée » du point de vue de l'emploi n'est pas exempte de tensions ponctuelles. D'abord à cause de la relative « pénurie » de spécialistes formés en sécurité informatique, mais également, dans un contexte de fort « *turn over* » des jeunes ingénieurs de l'ANSSI, qui, une fois formés, sont débauchés par le privé notamment, de **la règle (non écrite ?) tendant à ce que tout poste vacant au 31 décembre soit considéré comme devant être supprimé, qui oblige parfois l'Agence à devoir « défendre » en pratique des postes qui lui ont pourtant été accordés en loi de finances.**

Avec ce fort « turn over » de ses cadres, très bien formés, l'Agence participe à l'essaimage de la culture « cyber » dans les différents secteurs de l'économie.

ÉVOLUTION DES EMPLOIS DE L'ANSSI DEPUIS 2008

Emplois ANSSI	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**
Effectifs au 1/1/N (en ETP)	**110**	122 *	132	172	212	292	357	422	**487**
Evolution annuelle (en ETP)	**12**	**10**	**40**	**40**	**80**	**65**	**65**	**65**	
		* Effectif de la DCSSI, prédecesseur de l'agence.							

Source : réponse du Gouvernement au questionnaire de votre commission

Du point de vue des crédits de **développement**, d'équipement et de fonctionnement, ils enregistrent, dans un souci de maîtrise de la dépense publique, une **diminution de 1% des crédits de paiement.**

Au total, l'évolution des crédits de l'ANSSI depuis 2009 montre bien à la fois la montée en puissance des moyens de l'Agence engagée ces 5 dernières années, mais également la relative décrue tendancielle de cette augmentation en 2015 :

ÉVOLUTION DES CRÉDITS DE L'ANSSI DEPUIS 2009

Crédits HT2 ANSSI (en M€)	**AE**	**CP**	**Evolution annuelle CP**
LFI 2009	29,58	25,33	
LFI 2010	35,76	32,52	28%
LFI 2011	47,93	47,32	46%
LFI 2012	68,88	55,81	18%
LFI 2013	67,25	67,32	21%
LFI 2014	63,35	69,66	3%
PLF 2015	58,98	68,99	-1%

Source : réponse du Gouvernement au questionnaire de votre commission

Ces ressources sont destinées à financer les **projets innovants** - dont les programmes interministériels PMPS (plan de modernisation des produits de sécurité gouvernementaux) et CNG (cryptophonie de nouvelle génération) - de développement et de mise en œuvre d'une part des moyens de communication sécurisée gouvernementale et intergouvernementale, dont ceux exploités par le Centre de transmission gouvernemental (CTG), et d'autre part des moyens de protection informatique des réseaux sensibles de l'Etat 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, compte tenu de la croissance des effectifs (implantations des Invalides et Tour Mercure). L'extension des besoins de moyens techniques de l'ANSSI nécessite en effet le développement d'espaces climatisés informatiques type « *Data center* » (salles de serveurs) au-delà de ces implantations.

Par ailleurs, des crédits seront **transférés vers le ministère de la défense** au titre des projets interministériels :

- 4,5 millions d'euros d'autorisations d'engagement et 6,8 millions d'euros de crédits de paiement au titre du plan interministériel de modernisation des produits de sécurité gouvernementaux précité (PMPS) ;

- 0,4 million d'euros d'autorisations d'engagement et 1,9 million d'euros de crédits de paiement au titre du programme lancé en 2012 de « chiffreurs souverains » ;

- 0,9 million d'euros d'autorisations d'engagement et 4,4 millions d'euros de crédits de paiement au titre du programme de cryptophonie de nouvelle génération (CNG) ;

- 59,9 millions d'euros d'autorisations d'engagement et 81,2 millions d'euros de crédits de paiement pour les besoins en capacités techniques interministérielles (CTIM).

3. Un renforcement qui reste modeste au regard des moyens consacrés à la cyberdéfense par nos principaux partenaires et alliés

Nos principaux partenaires et alliés ont une organisation sensiblement différente de la nôtre en matière de cyberdéfense, qui rend toute comparaison internationale difficile.

Il est néanmoins possible de retenir les quelques grands enseignements suivants :

• le *Bundesamt für Sicherheit in der Informationstechnik* (BSI) allemand, dont des missions recouvrent celles de l'ANSSI, a actuellement un effectif de **580 ETP**. Le budget du BSI est comparable à celui de l'ANSSI ;

• l'organisation de ces missions au Royaume-Uni rend plus difficile la comparaison mais on peut estimer qu'environ **800 personnes** évoluent dans des structures dont la mission recouvre une partie de celles de l'ANSSI ;

• 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 1 000 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.

COMPARAISON INTERNATIONALE DES AGENCES CHARGÉES DE LA CYBERDÉFENSE

	France	**Allemagne**	**Etats-Unis**	**Royaume-Uni**
Pilotage de la mise en œuvre de la stratégie de cybersécurité	ANSSI	BMI	Maison Blanche (EOP/NSC)	OCSIA
CERT gouvernemental	ANSSI	BSI (Cert-Bund)	DHS (US-CERT)	GCHQ (GovCERT-UK)
Gestion opérationnelle des incidents de cyberdéfense	ANSSI	BSI (administrations seulement)	NSA (NTOC)	GCHQ (Direction Cyber)
Gestion des sondes de détection gouvernementales	ANSSI	BSI	DHS (programme Einstein)	GCHQ (Direction Cyber)
Soutien technique pour les opérateurs d'infrastructures critiques	ANSSI	BSI	DHS	MI-5 (CPNI)
Coordination de la cyberdéfense opérationnelle au niveau gouvernemental	ANSSI	BSI (NCAZ)		CSOC (plate-forme de coordination interministérielle hébergée au GCHQ)
SSI dans les réseaux classifiés (dont cryptologie)	ANSSI	BSI	NSA	GCHQ (CESG)
Evaluation de produits (protection du sensible non classifié)	ANSSI (Centre de Certification, Critères Communs) DGA	BSI (Centre de Certification, Critères Communs)	NSA (Centre de Certification, Critères Communs)	GCHQ (CESG)
Agrément de produits (protection du classifié)	ANSSI	BSI	NSA	GCHQ (CESG)
Existence d'un accès unifié et sécurisé des administrations à internet	RIE (en cours)	OUI	NON	OUI
Effectif	**424 Fin 2014**	**582**	**Plusieurs milliers**	**800 (Estimation)**

Source : Réponse du Gouvernement au questionnaire budgétaire de votre commission

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).

L'évolution budgétaire pour ces établissements (avec une baisse de la contribution de l'Etat) applique les orientations générales du Gouvernement qui se traduit en 2015 par une diminution de 2% du montant de la subvention aux opérateurs de l'Etat. L'effort d'économie demandé à ces deux instituts est un facteur supplémentaire de recherche de synergies et de mutualisations entre ces deux établissements de formation co-localisés à l'Ecole militaire à Paris.

Par ailleurs, cette action contient la dotation en fonds spéciaux des services spécialisés de renseignement et ceux de l'Académie du renseignement.

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

L'Institut des hautes études de la défense nationale (IHEDN) constitue un **pôle public de référence pour la formation à la stratégie de défense et de sécurité nationale**. Acteur institutionnel d'influence, c'est un lieu d'échange et de réflexion irremplaçable au sein de la Nation pour sensibiliser, former et faire rayonner l'esprit de défense.

1. Une modernisation engagée, une priorité à la formation des jeunes générations

L'IHEDN est engagé dans un processus de **modernisation**. En particulier, le « *projet d'établissement 2020* » a vocation à décliner les domaines et finalités des activités de cet organisme de formation et d'études, ainsi que les **partenariats** à développer, notamment avec l'Institut national des hautes études de la sécurité et de la justice (INHESJ). Une priorité est donnée à la formation des **jeunes professionnels** et des élus ainsi qu'au renforcement des actions en **région**. Ce projet doit fixer également les priorités de modernisation de l'organisation et de rationalisation de la gouvernance de l'Institut ainsi que le renforcement des financements externes et des ressources propres.

L'Institut augmentera ainsi dès 2015 le nombre de séminaires destinés aux **jeunes générations**. Son offre passera ainsi de 4 à 6 séminaires par an, avec une augmentation de 5% du nombre de jeunes sensibilisés. Cet effort de formation viendra compléter l'offre actuelle à destination de la

jeunesse au travers des séminaires « Grandes écoles », « Master 2 » et « Ecole polytechnique ».

En 2015, pour l'ensemble des formations, **plus de 700 jeunes** seront ainsi formés par l'Institut. La priorité sera également donnée, à côté des formations nationales, aux formations en région, notamment auprès des jeunes professionnels et des élus.

Certaines initiatives montrent le **dynamisme** de l'IHEDN, qu'il s'agisse des « Lundis de l'IHEDN », où de grands témoins interviennent, et qui rencontrent un vif succès, ou encore des « Débats de l'actualité » centrés sur des thèmes d'actualité, en partenariat avec un quotidien de la presse écrite.

Vos rapporteurs soutiennent l'Institut dans sa volonté de diversifier son recrutement et de renforcer l'action de chaque auditeur, ou ancien auditeur, pour s'engager et rayonner au-delà même de sa participation aux formations de l'IHEDN.

2. Des ressources sous contrainte

La rationalisation de la gouvernance de l'Institut est également engagée, dans un objectif de maîtrise de la dépense publique et de réduction du coût des activités et du fonctionnement.

La totalité de la subvention à l'IHEDN s'élevait dans le projet de loi de finances pour 2014 à **8,545 millions d'euros**, ramenés à **8,351 millions** d'euros après mise en réserve.

Le montant total des recettes et des dépenses du budget initial 2014 s'élevait à 10,253 millions d'euros. La loi de finance rectificative d'août 2014 a prévu une réduction des crédits de l'Etat à hauteur de 321 000 euros pour la subvention pour charges de service public de l'IHEDN.

L'équation budgétaire demeure donc sous tension : l'IHEDN doit trouver des **recettes extérieures** (droits d'inscription, partenariats, mécénats, taxe d'apprentissage) et faire preuve de **maîtrise dans les dépenses**, tout en poursuivant la **décrue de ses effectifs**.

Les ressources propres de l'IHEDN

Les ressources propres de l'IHEDN, d'un montant de 1,999 million d'euros, sont composées de la façon suivante :

- recettes en provenance de l'Etat (783 K€) :

. remboursement par le ministère de la défense des frais de formation des sessions nationales « Armement et économie de défense » (138 K€) ;

. contribution du ministère des affaires étrangères/DCSD pour les formations à l'international relatives à la politique de défense (553 K€) ;

. contribution du ministère de la défense/DGA/DI pour les formations à l'international relatives à l'armement et économie de défense (66 K€) ;

. contribution du ministère de la défense pour les formations SERA et CESD (26 K€).

- recettes propres concernant les frais d'inscriptions des auditeurs aux sessions nationales, régionales ainsi qu'aux autres formations et prestations de sensibilisation (1 122 K€).

- des recettes diverses (94 K€).

A ces ressources propres, il faut rajouter 90 000 € de taxe d'apprentissage.

Source : réponse du Gouvernement au questionnaire budgétaire de la commission

Dans le projet de loi de finances pour 2015, **la subvention pour charges de service public** inscrite au sein du programme 129 s'élève à **8,226 millions d'euros**. Comme pour les autres opérateurs de l'Etat, l'IHEDN supporte une diminution de 2% par rapport à 2014 ; en outre quatre emplois ont été supprimés mi-2014.

Le montant total des recettes et dépenses de l'IHEDN prévu pour 2015 s'élève à **10,115 millions d'euros, soit une diminution de 1,3**% par rapport à son budget initial en 2014.

BUDGET DE L'IHEDN EN 2015 (EN MILLIERS D'EUROS)

Recettes	Montants prévisionnels	Dépenses	Montants prévisionnels
Dotation de l'Etat	**8 544**	**Activités**	**2 183**
Suppression 2 ETP	-148	**Fonctionnement de la structure**	**7 932**
		dont fonctionnement courant	*850*
Effort dépenses de fonctionnement	-171		
Total subvention (budget triennal)	**8 225**		
Total subvention (lettre de cadrage)	**8 225**		
Mise en réserve	-199		
Total subvention après mise en réserve	**8 026**		
Ressources propres	1 999		
Taxe d'apprentissage	90		
	10 115		**10 115**

Source : réponse du Gouvernement au questionnaire budgétaire de la commission

3. Des effectifs en baisse

En 2015, le plafond d'emploi annuel sera de 96 équivalents temps plein travaillés (ETPT), soit une diminution de **4 emplois** par rapport à la loi de finances pour 2014. D'après les informations recueillies par vos

rapporteurs[1], le schéma d'emploi pour 2015 se concrétisera effectivement par **une baisse de 2 emplois[2].**

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

1. Un institut en mutation, qui consolide son expertise en matière de formation sur la sécurité et la justice

L'Institut national des hautes études de sécurité et de justice (INHESJ) dispense des formations qui mettent particulièrement en exergue les liens forts qui existent entre sécurité, d'une part, et justice, libertés publiques et droit, d'autre part. L'Institut organise, depuis 2013, **trois sessions nationales réunissant 170 auditeurs** : « *Sécurité et justice* », « *Protection des entreprises et intelligence économique* », « *Management stratégique de la crise* », session nouvellement créée qui répond à un besoin exprimé par les hauts cadres des secteurs publics et privés souhaitant partager leurs expériences.

Outre ses publications reconnues, telles que les *Cahiers de la Sécurité et de la Justice*, des lettres mensuelles et des bulletins spécialisés, l'Institut abrite **l'Observatoire national de la délinquance et des réponses pénales (ONDRP),** organisme unique dans l'étude et l'analyse des évolutions statistiques de l'ensemble du processus pénal et des phénomènes criminels.

La mise en œuvre d'un plan stratégique visant à conforter l'Institut et à adapter son organisation est prévue en 2015, dans le cadre d'une mutualisation accrue –notamment sur le plan des soutiens– avec l'IHEDN.

2. Une dotation budgétaire en baisse, compensée partiellement par l'augmentation des ressources propres

Les ressources de l'INHESJ sont composées en majeure partie de la subvention pour charges de service public portée par le programme 129, complétées par le produit des différentes formations et études réalisées par l'Etablissement. Une autre partie, plus marginale, des recettes, est constituée des produits des publications et de la perception de la taxe d'apprentissage.

---

[1] *Source : réponse au questionnaire budgétaire de la commission.*

[2] *Le Gouvernement indique que «En 2015, le plafond d'emploi annuel sera de 96 ETPT (- 4 ETPT/ LFI 2014). Le schéma d'emploi arbitré pour 2015 est de -2 ETP. Le plafond d'emploi intègre ce schéma en année pleine (-2 ETPT), auquel s'ajoute une correction technique (-2 ETPT) liée à 2 emplois d'ouvriers d'Etat de l'ex-Centre des hautes études de l'armement (service de la DGA) intégrés sous plafond de l'établissement public en PLF 2010 lors de l'intégration de ce service au sein de l'IHEDN et qui relèvent dorénavant des « autres emplois rémunérés par l'Etat par d'autres programmes ».*

En 2014, le montant de la contribution du budget s'est élevé à **9,4 millions d'euros**, ramenés à **9,1 millions d'euros** après mise en réserve. La loi de finances rectificative d'août 2014 a prévu une réduction de crédit à hauteur de 261 000 euros.

Ces réductions sont en partie compensées par une augmentation des **ressources propres de l'Institut**, en particulier celles associées à ses capacités de formation et d'étude, qui se stabilisent **à hauteur de 1,5 million d'euros, soit actuellement 12% du montant total des recettes**.

Parallèlement, l'Eablissement s'attache à poursuivre sa politique de contraction de ses dépenses, tant par des mesures de mutualisation et de groupement d'achats, que par une politique interne restrictive en matière de dépenses.

L'Institut va supporter, à l'instar des autres opérateurs de l'Etat, des réductions de 2% par an. Les efforts de réduction des dépenses de fonctionnement seront donc maintenus. Dans ce contexte, la subvention inscrite au projet de loi de finances pour 2015 s'élève à **9,2 millions d'euros.**

EFFECTIFS DE L'INHESJ

	Plafond d'emploi		Hors plafond d'emploi		Total	
	ETP	**Réalisé**	ETP	Réel	ETP	Réel
31/12/2013	**83**	**75**	8	6	91	81
30/06/2014	**79**	**76**	8	8	87	84

ETP : équivalent temps plein. Source : réponse du Gouvernement au questionnaire de la commission

C. LE RAPPROCHEMENT ENGAGÉ ENTRE L'IHEDN ET L'INHESJ

L'IHEDN et l'INHESJ sont engagés dans un processus de rapprochement qui se matérialise notamment par la **mutualisation des fonctions de soutien**, en application d'une convention cadre, qui se traduit par :

- la mise en place de procédures communes dans le domaine du recrutement, de la rémunération, des déplacements et de la commande publique ;

- des audits initiés en commun, la mise en place d'une architecture informatique commune, l'acquisition en commun de matériels et prestations communes avec partage des coûts ;

- la mise en commun des moyens d'impression et de publication ;

- la mise à disposition par l'IHEDN de locaux pour les ressources humaines et l'informatique pour faciliter les échanges entre le personnel, avec contribution aux charges au prorata de la surface occupée ;

- l'utilisation mutualisée des amphithéâtres et des salles de formation ;

- la mise en place d'un groupement de commande au 1er janvier 2014 pour certaines acquisitions. Un projet de création d'une agence comptable unique (IHEDN/INHESJ) est par ailleurs en cours.

Des synergies sont également recherchées dans le domaine **pédagogique** : **cinq séminaires communs** sont organisés entre les deux sessions nationales.

Votre commission ne peut qu'encourager ce processus, cohérent avec le continuum dégagé dès le Livre blanc de 2008 entre la sécurité et la défense nationales. Ce rapprochement devrait d'ailleurs se poursuivre en 2015 et déboucher sur de nouveaux champs, tant dans le domaine du soutien (agence comptable commune) que de la formation. Ces nombreuses actions de mutualisation s'inscrivent pleinement dans la démarche de réduction de la dépense publique.

Pour autant, il est souhaitable de veiller à conserver la personnalité propre, l' « ADN », de chacun des deux Instituts.

D. L'ACADÉMIE DU RENSEIGNEMENT

La création de l'Académie du renseignement, en 2010, est, avec la mise en place d'un Coordonnateur national placé auprès du Président de la République, l'une des mesures emblématiques du renforcement du renseignement en France à la suite du Livre blanc sur la défense et la sécurité nationale de 2008, et plus particulièrement de la constitution d'une véritable « **communauté du renseignement**[1] ».

Le décret de 2010 qui fixe les missions de l'académie en fait en effet la pierre angulaire du renforcement des liens entre les différents services.

Décret n°2010-800 du 13 juillet 2010

Art. 2. − L'académie du renseignement concourt à la formation du personnel des services de renseignement placés sous l'autorité des ministres chargés de la sécurité intérieure, de la défense, de l'économie et du budget, au renforcement des liens au sein de la communauté française du renseignement ainsi qu'à la diffusion de la culture du renseignement.

À ce titre, elle a notamment pour mission :

– de concevoir, d'organiser et de mettre en œuvre des activités de formation initiale et continue au profit du personnel des services mentionnés au premier alinéa ;

– de favoriser la coopération entre ces services en matière de formation ;

– de participer aux actions de sensibilisation au renseignement.

[1] *Comprenant, autour du Coordonnateur national du renseignement, six services (DGSE, DGSI, DRM, DPSD, DNRED et TRACFIN).*

L'Académie du renseignement est d'une certaine manière devenue le symbole du renforcement des liens au sein de la communauté du renseignement, à travers l'offre de formations communes et la constitution d'une culture partagée.

Plus précisément, l'Académie organise différents types de formations :

. une formation initiale pour tous les cadres nouvellement affectés au sein des six services de renseignement. Son objectif est de leur permettre de comprendre le monde du renseignement dans lequel ils entrent et de se connaître. Elle a pour ambition de les amener à réfléchir au rôle et à la place du renseignement dans un pays démocratique comme la France et de leur faire prendre conscience de la spécificité de leur mission, au service de l'intérêt général ;

. des séminaires spécialisés, modules courts sur des thématiques précises à destination des cadres des services de renseignement. Sans se substituer aux formations internes ou aux éventuelles coopérations bilatérales, ces modules prolongent l'esprit de la formation initiale, en permettant un approfondissement des connaissances et une réflexion partagée sur des sujets d'intérêt commun et des problématiques ciblées ;

. un cycle supérieur du renseignement, destiné à une vingtaine d'auditeurs, cadres à haut potentiel des services de renseignement, conçu pour être compatible avec des responsabilités professionnelles de haut niveau. Ce cycle privilégie un contenu et des méthodes centrés sur l'expérience concrète par la mise en relation des auditeurs avec des décideurs, des témoignages de personnalités, le partage d'expérience, des visites sur le terrain et des rencontres.

Le nombre de personnes formées par l'Académie depuis 2010 est de l'ordre du millier[1].

Outre ces actions de formation des cadres des services**, elle a également été la cheville ouvrière de la rencontre avec les directeurs de services organisée en juillet dernier à l'attention des Parlementaires.**

Cette mission de diffusion de la culture du renseignement, notamment par des **actions de sensibilisation au renseignement** ainsi que des **manifestations publiques** (colloque, rencontres, etc.) et de **communication paraît tout à fait essentielle**.

Plus généralement, l'Académie vise à développer sa visibilité auprès du monde universitaire et des publics extérieurs à la communauté du renseignement, intéressés par cette thématique.

Du point de vue de son effectif et de son budget, l'académie du renseignement est une petite structure très légère. Ses crédits sont issus d'un

[1] *Source : réponse au questionnaire budgétaire de votre commission.*

redéploiement de crédits dévolus initialement aux services de renseignement et son budget de fonctionnement s'élevait en 2011 à 445 525 euros, en 2012 à 489 000 euros, et en 2013 à 444 000 euros. **En 2014, les crédits de fonctionnement ont été baissés de 10%, à 399 600 euros[1], pour tenir compte de la réalité des dépenses de l'Académie à ce stade de son développement.**

Les crédits de personnel (12 emplois, dont la directrice, son adjoint, et 4 conseillers pédagogiques) s'élèvent quant à eux à **845 713 euros**.

Cette sobriété budgétaire est à relever, dans un contexte où les missions de l'Académie ont monté en puissance à rythme soutenu.

En raison du développement des activités, il paraîtrait souhaitable que les crédits de fonctionnement soient désormais maintenus à ce niveau.

E. LES FONDS SPÉCIAUX

1. Une enveloppe de 50,2 millions d'euros

Les fonds spéciaux sont consacrés au financement de diverses actions liées à la sécurité extérieure et intérieure de l'Etat. Ils s'élèvent à **50,2 millions d'euros** en autorisations d'engagement et en crédits de paiement dans le projet de loi de finances pour 2015[2]. Ils concernent les services de renseignement, et en particulier la direction générale de la sécurité extérieure du ministère de la défense, ainsi que le Groupement interministériel de contrôle (GIC).

Créé par décret n° 2002-497 du 12 avril 2002, le groupement interministériel de contrôle (GIC) est un service du Premier ministre chargé des interceptions de sécurité. Les crédits du groupement interministériel de contrôle couvrent notamment des dépenses de personnel et de fonctionnement courant de l'organisme, ainsi que la rémunération des prestations fournies par les opérateurs de téléphonie mobile. Seules les dépenses à caractère sensible du GIC sont financées par des fonds spéciaux.

2. La réforme de la composition de la Commission de vérification des fonds spéciaux par la loi de programmation militaire du 18 décembre 2013

La loi de programmation militaire du 18 décembre 2013 a modifié la composition de la Commission de vérification des fonds spéciaux (CVFS).

Dans le cadre plus général d'un approfondissement du contrôle parlementaire sur les services de renseignements, la CVFS est désormais une

---

[1] *Source : réponse au questionnaire budgétaire de votre commission.*

[2] *Source : projet annuel de performance.*

formation spécialisée au sein de la délégation parlementaire au renseignement.

La CVFS est composée de **deux députés et de deux sénateurs**, membres de la délégation parlementaire au renseignement, désignés de manière à assurer une représentation pluraliste. Le président de la commission de vérification est désigné chaque année par les membres de la délégation. C'est le président de la commission des affaires étrangères, de la défense et des forces armées du Sénat qui en assure la présidence depuis l'entrée en vigueur de la loi en février 2014.

L'article 13 de la loi de programmation militaire du 18 décembre 2013 a également prévu que le rapport de la CVFS « *est présenté aux membres de la Délégation parlementaire au renseignement qui ne sont pas membres de la commission* », ce qui permet d'atteindre en pratique l'objectif, porté notamment par votre commission lors de l'examen de la LPM, d'une unification des différentes facettes du contrôle parlementaire des services de renseignement.

EXAMEN EN COMMISSION

La commission, sous la présidence de M. Jean-Pierre Raffarin, a examiné le présent rapport pour avis lors de sa réunion du 26 novembre 2014.

Après l'exposé des rapporteurs, un débat s'est engagé.

Mme Marie-Françoise Perol-Dumont. – Quelles mesures prendre pour faire face à la pénurie que vous évoquez d'ingénieurs formés en cyber sécurité ?

M. Jean-Marie Bockel co-rapporteur. – L'Etat peut et doit donner une impulsion, faire passer des messages aux différentes écoles et lieux de formation concernés sur l'intérêt qu'ils ont à former des ingénieurs dans ce secteur, compte tenu des besoins et des débouchés. Sachons saisir cette opportunité.

M. Robert del Picchia, – Certains anciens « hackers » peuvent parfois présenter un profil intéressant pour le recrutement…

M. Jean-Marie Bockel co-rapporteur. – L'ANSSI a besoin de profils très qualifiés.

M. Jean-Pierre Masseret, co-rapporteur. – Le ministère de la défense constitue un pôle cyber en Bretagne, 1 milliard d'euros de crédits y seront consacrés sur la durée de la programmation. En tant que Président de la région Lorraine, je mesure tout l'intérêt de disposer d'un centre d'excellence comme le LORIA, dans le domaine civil, dont la région est d'ailleurs partenaire.

M. André Trillard. – Il est parfois difficile à certains services du ministère de la défense d'attirer des talents en cyber sécurité, avec des salaires qui sont parfois en dessous des offres dans le privé ou dans d'autres administrations.

M. Jean-Marie Bockel co-rapporteur. – L'ANSSI est attractive sur le marché des jeunes talents ; la fidélisation est plus difficile, mais, après tout, cela favorise l'essaimage d'une culture cyber dans l'économie. La création d'une filière, avec des allers-retours entre privé et public, n'a que des avantages. Pour les Ecoles et Universités, c'est un jeu gagnant-gagnant d'enrichir leur offre de formation en la matière car, encore une fois, il y a des débouchés.

M. Daniel Reiner. – La loi de programmation militaire a permis des avancées importantes pour progresser dans cette culture de la confiance qui est indispensable. Il était nécessaire en particulier de prévoir de partager l'information sur les attaques. Quel est le rôle de l'OTAN en matière de cyber défense ? Un partage entre alliés est-il envisageable ? Quel est le rôle

du Centre d'excellence de cyberdéfense de l'OTAN (CCDCOE) déployé en Estonie ?

M. Jean-Marie Bockel, co-rapporteur. – Nous nous heurtons à un problème de mentalités. Hier, quand un problème était décelé, la réaction était de ne pas en parler, en pensant -ce qui était d'ailleurs parfois vrai- que le révéler serait se pénaliser. Il faut raisonner à l'inverse : être attaqué, c'est avoir de la valeur ; détecter l'attaque, c'est être en capacité de le faire, dans un monde où l'attaque se banalise. Plusieurs attaques récentes chez des industriels ont duré des mois, voire des années, avant qu'on ne s'en aperçoive ! Plus vite on réagit, plus on limite les dégâts.

Le centre de l'OTAN de Tallin pourrait en quelque sorte être comparé à un « think tank » : il faut y participer, il est très utile d'établir des règles du jeu, d'impulser un état d'esprit commun, y compris d'ailleurs dans la dimension juridique. Dans notre rapport de 2012 nous avions toutefois relevé quelques anecdotes qui montraient que la culture de la protection n'était pas très élevée au sein même du Secrétariat général de l'Alliance ! La situation s'améliore, mais la principale difficulté reste le nombre de pays concernés. Certains de nos partenaires européens ne sont pas encore assez sensibilisés sur cette question. La difficulté du partage dans ce cas est que la sécurité de l'ensemble dépend de celle du maillon le plus faible…

Je pense personnellement qu'il sera nécessaire d'établir des règles internationales -pourquoi pas sous l'égide de l'ONU ?- car, même si elles ne sont pas appliquées immédiatement, elles auront tracé les limites. Tout pays les franchissant sera alors exposé à la sanction de l'opinion publique, car nous sommes dans un monde où tout finit toujours par se savoir : ce n'est pas neutre.

M. Jean-Pierre Raffarin, président. – La loi de programmation militaire a instauré une obligation de déclaration pour les opérateurs d'importance vitale : c'est une étape importante.

M. André Trillard. – La DPSD, direction de la protection au ministère de la défense, est dans la même problématique. On parle rarement de nos entreprises pourtant ultra-compétentes dans ce domaine, je pense à Dassault Systèmes par exemple…

M. Jean-Marie Bockel, co-rapporteur. – J'évoque quant à moi fréquemment nos grands champions -car nous avons la chance d'en avoir encore !- et qui contribuent d'ailleurs parfois à l'émergence de PME. Dassault Systèmes est un exemple, on pourrait aussi parler d'Alcatel Lucent, ou encore de Thalès.

À l'issue de ce débat, la commission décide, à l'unanimité, de donner un avis favorable à l'adoption des crédits de la mission « Direction de l'action du Gouvernement » dans le projet de loi de finances pour 2015.

ANNEXE I -
AUDITION DE M. LOUIS GAUTIER, SECRÉTAIRE GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE

Lors de sa séance du 4 novembre, la commission a auditionné M. Louis Gautier, Secrétaire général de la défense et de la sécurité nationale.

M. Jean-Pierre Raffarin, président. – Mes chers Collègues, nous poursuivons notre cycle d'auditions consacré à l'examen du projet de loi de finances pour 2015, en accueillant Louis Gautier, qui vient de prendre ses fonctions de Secrétaire général de la défense et de la sécurité nationale.

Monsieur le Secrétaire Général, nous connaissons tous la sensibilité et l'importance des missions du SGDSN, au cœur de nos préoccupations, qu'il s'agisse de lutte contre la prolifération, d'exportation de matériel de guerre, de planification en matière de défense et sécurité, de préparation et de gestion des crises graves, ou encore de sécurité des communications gouvernementales, et – j'aurais garde de l'oublier au sein de notre commission si impliquée sur ce sujet - de cyberdéfense.

Ebola, Vigipirate, les drones survolant les centrales nucléaires, la cyber : vous avez du pain sur la planche ! Je vous laisse donc sans plus tarder la parole pour que vous puissiez nous parler de vos perspectives, et de votre budget.

M. Louis Gautier, secrétaire général de la défense et de la sécurité nationale.- Je suis très heureux de cette audition diligentée par votre commission pour la deuxième année consécutive - la première fois pour moi depuis ma récente nomination. Elle est l'occasion d'un examen des crédits du SGDSN figurant dans le projet de loi de finances 2015 au programme 129 des services du Premier ministre. Le SGDSN est une institution qui a peu souvent l'occasion de s'exprimer publiquement sur ses missions. Je vous remercie donc de l'opportunité que vous m'offrez de le faire aujourd'hui.

J'ai trouvé en prenant mes fonctions une administration en bon ordre de marche, et je veux tout d'abord rendre hommage à mon prédécesseur Francis Delon, qui a présidé pendant 10 ans aux destinées du SGDSN. Le SGDSN, administration sans histoire quoiqu'au cœur de l'Etat, est insuffisamment connu du public. Peut-être faut-il en chercher la raison dans une certaine culture du secret, nécessaire à la réalisation et à la nature de ses missions. Le SGDSN agit en appui de la prise de décision politique : ses travaux n'ont pas forcément vocation à être portés sur la place publique. D'un autre côté, il lui faut aussi s'adapter aujourd'hui à certaines exigences de transparence, inhérente à la vie démocratique, et aux légitimes demandes de nos concitoyens d'évaluer mieux la performance des services de l'Etat. La Cour des comptes a d'ailleurs engagé ce mois-ci un contrôle de l'Agence nationale de sécurité des systèmes d'information, (ANSSI), rattachée au

SGDSN, et l'Inspection générale des finances doit rendre prochainement ses conclusions sur l'organisation des services du Premier ministre dont fait partie le SGDSN. Autrefois concentré sur son travail de coordination ministériel, le SGDSN doit aussi aujourd'hui veiller à l'élargissement d'une culture de protection et de prévention, par exemple en matière de sécurité informatique qui touche non seulement les services de l'Etat, mais au-delà les opérateurs privés, et également nos concitoyens. Ainsi, le futur plan « Ebola », ou le récent plan « Vigipirate » rénové ont vocation à être largement diffusés et connus du public : nous avons d'ailleurs déclassifié la grande majorité des mesures du plan Vigipirate à cette fin.

Le SGDSN a trois missions principales : d'abord un rôle de veille et d'alerte, pour ainsi dire de vigie, face aux menaces et aux risques. Ensuite, un rôle de « notaire public », à la fois conseil et rédacteur des décisions prises par l'Exécutif en matière de défense et de sécurité nationales. Enfin, un rôle d'opérateur, qu'il s'agisse de la gestion des habilitations, et des documents classifiés, des communications gouvernementales, ou encore de la sécurité des systèmes d'information cyberdéfense avec l'ANSSI.

Le SGDSN est organisé en quatre pôles, deux sont constitués en directions d'administration centrale : protection et sécurité de l'Etat (PSE) ; affaires internationales et stratégiques (AIST) ; un pôle est érigé en service à compétence nationale, l'ANSSI ; et deux établissements publics sont placés sous sa tutelle : l'Institut des hautes études de la défense nationale (IHEDN) et l'Institut national des hautes études de sécurité et de justice (INHESJ). S'y ajoute un service d'administration générale, qui assure le soutien ou le suivi administratif de cet ensemble.

Au sein du programme 129, les crédits prévus en 2015 s'élèvent à environ 243 millions d'euros en crédits de paiement, dont 94 millions sont transférés à la défense pour financer des programmes interministériels, notamment le renforcement des capacités techniques d'interception, de chiffrage et de décryptement. Par ailleurs, le budget du SGDSN porte les 17 millions, correspondant aux subventions affectées aux deux instituts précités. En termes de moyens humains, le nombre de postes en équivalents temps pleins s'élève à 850 personnels, dont à partir de cette année, 184 personnels affectés au centre de transmission gouvernementale (CTG) rattachés au SGDSN.

Ce budget 2015 est marqué par trois faits notables :

- la poursuite du plan de renforcement des moyens de l'ANSSI, qui disposera fin 2015 d'un effectif de 500 personnes, ce qui situera cette agence à un niveau, certes en deçà des moyens britanniques et américains mais comparable aux moyens allemands ;
- l'intégration du centre de transmission gouvernemental déjà mentionnée ;

- la contraction légère prévue au plan triennal des moyens du SGDSN et des deux instituts sous tutelle.

Avec les crédits budgétaires et les personnels qui lui sont rattachés, le SGDSN est en mesure d'exercer correctement les compétences et les responsabilités qui lui sont confiées. La direction protection et sécurité de l'Etat est chargée du suivi des crises, de la préparation des plans gouvernementaux et de l'organisation de l'Etat en temps de crise. En son sein, un bureau spécifique fonctionnant 24h/24 est relié à l'ensemble des cellules de crise dans tous les ministères et il les alimente de notes de situation et de synthèse. Il a ainsi permis de diffuser des informations aux administrations centrales et décentralisées lors de l'intervention au Mali, de l'accident de la Malaysian Airlines ou encore au sujet de l'épidémie Ebola. J'envisage de réaliser un audit de satisfaction des organismes abonnés à ce service pour mieux répondre à leurs attentes et éventuellement d'en étendre la diffusion aux opérateurs qui ne sont pas aujourd'hui destinataires de nos productions, ainsi qu'aux services déconcentrés de l'État. La direction PSE contribue également à l'élaboration des projets de loi et des textes réglementaires dans le domaine de compétence du SGDSN : la récente loi anti-terrorisme, la mise en application de la loi de programmation militaire s'agissant de la cyberdéfense, la problématique du contrôle des services de renseignement, ou encore la question du fichier PNR (*Passengers Name Record*) dont l'un des décrets est publié et l'autre est en cours de validation interministérielle. Cette direction a enfin une mission générale d'actualisation de la planification, qu'il s'agisse de l'importante réforme de Vigipirate, conduite en 2014, - dont il faudra sans doute adapter la mise en œuvre car, des préfets, remonte un besoin de meilleur croisement de l'information et des instructions, au niveau du département - ou de la préparation actuelle, à partir du plan de pandémie grippale de 2011, d'un plan interministériel de lutte contre la fièvre Ebola. Le SGDSN a également pour mandat de réfléchir à l'évaluation des vulnérabilités face aux récents survols de drones au-dessus des centrales nucléaires. Face à la multiplication des intrusions, il est en train d'élaborer une réponse, tant juridique que capacitaire.

Le deuxième pôle, l'ANSSI, exerce, outre une fonction de veille permanente, un rôle décisif dans l'élaboration des normes en matière de cyberdéfense. Cette agence développe aussi un grand nombre d'outils et de procédés techniques permettant de détecter et de corriger les vulnérabilités des systèmes informatiques. Une visite de l'ANSSI vous permettrait de découvrir que le profil des salariés de l'agence est caractérisé par l'expertise et la jeunesse. L'âge moyen des personnels de l'ANSSI est de 28 ans. Au-delà de son assistance aux administrations de l'État, pour secourir leurs systèmes informatiques, l'Agence a développé un dialogue avec les opérateurs d'importance vitale sur lesquels repose aussi le bon fonctionnement des services publics et de l'économie. Le rôle crucial de l'ANSSI s'exerce non seulement auprès des administrations (avec le déploiement par exemple du

réseau crypté ISIS) mais aussi des opérateurs, il s'étend en outre au développement d'une véritable culture de sécurité informatique dans la société – en formant par exemple 1400 stagiaires cette année. L'ANSSI a aussi des fonctions de représentation internationale – je pense notamment à l'Union européenne et à l'OTAN – Ce n'est donc pas une agence purement technique. L'ANSSI a une responsabilité de coordination interministérielle et d'encadrement normatif, ce qui justifie pleinement son rattachement au Premier Ministre.

Le troisième pôle, affaires internationales et stratégiques, assure comme les deux autres, des missions de veille, de coordination et de contrôle. AIST effectue des synthèses de situation sur les grandes crises internationales (Libye, Mali, Syrie, Irak…), cette direction suit les négociations en matière de prolifération nucléaire (Iran…), ainsi que la mise en œuvre des grands traités de désarmement, comme par exemple la convention internationale d'interdiction des armes chimiques ou la participation à la coordination des signalements concernant la prolifération. Cette direction assure le pilotage de notre politique d'exportation d'armement et actualise en ce moment les « directives de haut niveau » qui servent de cadre méthodologique aux décisions proposées à l'exécutif, par la commission interministérielle pour l'étude des exportations de matériels de guerre, la CIEEMG. Ce travail très important doit concilier deux impératifs : ne pas entraver les activités industrielles tout en veillant à ce que l'exportation de matériels sensibles ne constitue pas une menace pour la paix et la sécurité de notre pays. Le CIEEMG tient 17 réunions plénières par an, a traité environ 7 000 dossiers ces 18 derniers mois, soit un flux mensuel de 400 autorisations. Grâce à la réforme que vous avez votée en 2011, le nouveau dispositif de contrôle a été mis en place, avec de nouvelles procédures de licences, rénovées, et des moyens informatiques modernisés favorisant la dématérialisation des traitements.

La dernière mission du SGDSN est d'exercer la tutelle de l'Institut des hautes études de la défense nationale, l'IHEDN et de l'Institut national des hautes études de la sécurité et de la justice, l'INHESJ, deux instituts qui ont pour vocation de former et sensibiliser respectivement aux questions de défense, de sécurité et de justice. L'IHEDN, au travers de ses sessions nationales, régionales et jeunes, touche chaque année 2 000 personnes. L'INHESJ, par ses sessions et ses séminaires, sensibilise 1 200 personnes chaque année. Chacun des deux instituts bénéficiera de 9 à 10 millions d'euros de budget en 2015.

M. Jean-Pierre Raffarin, président. – Merci monsieur le Secrétaire général. Je donne la parole à nos deux rapporteurs, MM. Jean-Marie Bockel et Jean-Pierre Masseret.

M. Jean-Marie Bockel, co-rapporteur. – Mes questions seront centrées sur la cyberdéfense mais nous évoquerons également la prévention de la radicalisation, sujet qui nous préoccupe dans les territoires. Je tiens à

saluer la présence du nouveau directeur de l'ANSSI avec lequel nous avons déjà eu l'occasion de travailler. Ainsi donc, en matière de cyberdéfense, l'article 22 de la loi de programmation militaire qui concerne les opérateurs d'importance vitale attend encore son décret d'application, puis les arrêtés sectoriels, pour entrer pleinement en vigueur. Quel est le calendrier envisagé pour leur publication ? Les grands opérateurs, au premier rang en matière de télécom ou d'énergie coopèrent-ils bien et dans de bonnes conditions, car c'est un concept un peu nouveau en France ? Ont-ils suffisamment intégré qu'ils y ont tout intérêt ? Pouvez-vous nous dire également comment favoriser la diffusion de la culture « cyber » qui permet de prévenir 90% des difficultés dans le tissu des entreprises privées et en particulier dans les PME, dans les ministères au-delà de la sphère « sécurité défense » ? Comprend-on que l'on a intérêt à signaler les incidents et les difficultés ? Cela bouge-t-il dans les ministères où des attaques ont parfois défrayé la chronique ? Quel peut être le rôle du Premier ministre et de ses services en faveur de cette diffusion ? Enfin pour terminer, l'ANSSI, sous la tutelle du SGDSN, ne cesse de croître en effectifs et en moyens. Quelle est la cible in fine, à quel format stable voyez-vous l'ANSSI à terme et où se situerait ce terme ? Le ministre de la défense a affiché des ambitions, laissant entendre que la mise à niveau irait plus loin que l'alignement avec nos grands voisins. Le rattachement de l'ANSSI au SGDSN apparaissait comme une bonne formule en son temps, « gagnant-gagnant ». Est-on toujours dans ce schéma ?

M. Jean-Pierre Masseret, co-rapporteur. – Vous avez évoqué le survol des centrales nucléaires par des drones. Qu'en sait-on ? Peut-on en parler ? Qu'y-a-t-il derrière tout cela ? Par ailleurs, la CIEEMG est au sein du SGDSN l'organe qui autorise les exportations d'armement. Quel bilan tirez-vous de la modernisation des procédures d'instruction que nous avons votée en 2011, et qui produit ses pleins effets – notamment avec un nouveau logiciel – cette année ? Je ne vous interrogerai pas sur le Vladivostock… Dernière question, le SGDSN a reçu un mandat d'étude sur la prévention de la radicalisation. Quels sont les résultats de ce groupe de travail ? Nous venons de durcir l'aspect répressif, avec la loi anti-terrorisme, mais qu'en est-il du volet préventif ?

M. Louis Gautier, secrétaire général de la défense et de la sécurité nationale.- Si vous m'y autorisez, je prendrai les questions dans l'ordre inverse de leur formulation. S'agissant du rattachement de l'ANSSI au SGDSN, les délégations de compétences qui lui sont accordées, par exemple en matière normative ou son rôle dans la coopération internationale, justifient par son positionnement actuel. Ce n'est donc pas simplement une agence technique. Sur la question de l'augmentation des moyens, je rappellerai d'abord que, dans notre pays, il y a une division radicale entre les moyens consacrés à la cyberdéfense et les moyens dont le ministre de la défense dispose pour protéger les systèmes militaires, mais aussi pour répondre à d'éventuelles agressions. Dans les pays anglo-saxons, un choix

différent a été fait. En France, cette démarcation s'explique au nom du respect des libertés publiques, mais aussi en raison de la mission de l'ANSSI qui s'étend au conseil à des opérateurs privés. Cette séparation à la fois organique et fonctionnelle me paraît valide et prouvée dans les faits. Nous avons programmé les effectifs de l'ANSSI pour atteindre 500 en 2015 et 600 en 2017, ce qui paraît suffisant pour assurer la stabilité de l'ANSSI, permettre des recrutements réguliers et le renouvellement souhaitable des personnels, qui participe de l'essaimage de la culture cyber dans la société. Nous pensons donc que nous aurons atteint en 2017 le bon étiage. Vous m'avez interrogé sur les secteurs que nous devrions davantage sensibiliser à la cyberdéfense. C'est une tâche parfois difficile. Il faut changer les habitudes. Nous portons la responsabilité de convaincre davantage. Le secteur de la santé par exemple ne se sent pas aussi concerné qu'il serait souhaitable par les enjeux de la cybersécurité. Or, la protection des données personnelles des dossiers médicaux mérite attention. La recherche a l'habitude d'un travail ouvert du fait notamment des exigences de coopération internationale, mais parfois il est aussi important que certaines opérations ne soient pas éventées, quand il s'agit de brevets par exemple. Il faut aider ces deux milieux à s'approprier, dans leur intérêt, les exigences de la culture du cyber. S'agissant de l'article 22, les décrets devraient être publiés en fin d'année et les arrêtés sectoriels tout au long de l'année 2015. Je propose que Guillaume Poupard, directeur général de l'ANSSI, vous fasse part de cet aspect de coopération avec les entreprises et les différents acteurs.

M. Guillaume Poupard, directeur général de l'ANSSI.- L'article 22 de la loi de programmation militaire fait que la France est le seul pays qui protège, par la loi, les opérateurs d'importance vitale, en imposant la mise en place des règles de sécurité définies par l'ANSSI, la remontée d'informations de la part des victimes d'attaques afin de donner l'alerte, de voir s'il y a d'autres attaques simultanées et de les aider à y répondre. Cet article permet également à l'ANSSI d'effectuer des contrôles sur les opérateurs en vue de vérifier que les moyens de sécurisation sont réellement mis en place et là, nous sommes dans le domaine règlementaire. Enfin cet article nous permet, en cas de crise majeure, comme celle subie par l'Estonie en 2007 avec une paralysie du pays, de donner des consignes strictes aux opérateurs afin de limiter, dans l'urgence, les conséquences de ces attaques. S'agissant du calendrier, nous sommes en « *courte finale* » pour les décrets d'application. Dans les différents domaines comme le transport, la défense, il y en a environ 18, nous allons définir des règles de sécurité et les différentes modalités d'application de la loi en coopération avec les opérateurs. L'ANSSI définit avec les différents opérateurs des règles applicables et soutenables, notamment sur le plan humain et financier. Ce travail est à même de rassurer les opérateurs qui voient que l'on travaille à leur sécurité en même temps qu'à celle de la Nation. Les arrêtés fixant ces règles sortiront au fil de l'eau en 2015. C'est un gros travail, mais je suis optimiste sur son issue. Nous sommes le premier pays au monde à entreprendre cette démarche, mais cet

article de loi suscite l'intérêt en Allemagne, qui rédige actuellement une loi en ce sens, et plus largement en Europe. En termes de diffusion de ces questions de cyber, nous nous sommes intéressés d'abord aux réseaux des ministères et de l'administration – et c'est toujours le cas –. L'article 22 a permis l'extension aux opérateurs d'importance vitale et donc aux entreprises privées, mais il va falloir aller plus loin et protéger toutes les cibles potentielles contre les attaques cyber, le domaine industriel et le domaine de la recherche. Le domaine croît de manière exponentielle et il va falloir y adapter nos moyens. On ne peut pas travailler avec les opérateurs d'importance vitale comme avec les PME. Nous avons un lien direct avec les opérateurs, alors que nous sommes davantage dans une démarche de conseils à l'égard des PME, auxquelles nous diffusons déjà des guides de bonnes pratiques et des conseils. Nous sommes également dans une stratégie de démultiplication de l'effort avec la qualification de prestataires privés capables de détecter des incidents et de sécuriser des réseaux. Nous créons ce faisant de nouveaux métiers liés à la cybersécurité, pour permettre aux gens de se défendre et de se trouver en situation de cybersécurité acceptable. Je signalerai que l'ANSSI n'est pas le seul acteur, c'est une démarche interministérielle. Nous avons des liens étroits avec le ministère de la défense, de l'intérieur, des affaires étrangères et de l'économie. S'agissant de la sécurité des ministères en général, il y a une très forte hétérogénéité dans le traitement des menaces informatiques. Le ministère de la défense est un des seuls à atteindre un niveau « mature ». Nous travaillons avec eux au quotidien, puisque leur centre opérationnel est co-localisé avec le nôtre. Des arbitrages devront être pris en termes d'allocation de ressources dans certains ministères car la cybersécurité a un coût. S'agissant du format, nous avons aujourd'hui les moyens de répondre à notre mission. Pour moi, ce sont les hommes qui comptent. Nous gérons le *turnover* mais nous n'avons pas de marge. S'agissant de la coopération, c'est un domaine de souveraineté. La matière à échanger est très sensible, si bien qu'elle prend plutôt la forme de liens bilatéraux dans lesquels peut s'installer une relation de confiance. Nous en avons par exemple avec le Royaume-Uni et nous y travaillons avec l'Allemagne. Il faut un intérêt à se défendre ensemble.

M. Louis Gautier, secrétaire général de la défense et de la sécurité nationale.- Vous m'avez interrogé sur la modernisation des procédures en matière d'exportations d'armements. J'ai déjà évoqué les 400 dossiers examinés par mois et les 2 500 licences déjà notifiées depuis la mise en place du nouveau régime. A ce stade, le bilan sur la mise en œuvre de SIGALE (Système de gestion et d'administration des licences d'exportation) est en demi-teinte. SIGALE doit être amélioré pour corriger certains dysfonctionnements (moteurs de recherche, traitement des rectificatifs demandés par les industriels), de finaliser les fonctionnalités attendues (signature électronique, etc.). Des améliorations sont donc nécessaires en termes de sécurisation du système et de rapidité. Sur la radicalisation, vous venez de voter un texte qui devrait faire avancer les choses de manière

substantielle. En ce qui concerne l'aspect de la prévention et de la détection, la mise en place du numéro vert a été une bonne chose. Par la chaîne des préfets, des recteurs, nous avons fait passer des messages pour intervenir suffisamment en amont dans le traitement des cas individuels de radicalisation. De la même façon, l'administration pénitentiaire est très sensibilisée au problème. Nous avons également développé des actions de coopération internationale avec les pays de départ et les pays de transit. Mais nous avons conscience des difficultés dues à la diffusion de la propagande sur Internet. Les idées combattent les idées et la meilleure arme est sans doute la force des convictions qui animent les éducateurs et les responsables à tous niveaux.

M. Robert del Picchia. – Il y a aussi l'intelligence économique, mais ce problème de cyberdéfense concerne toutes les entreprises. Vous avez évoqué la question de la santé. Je sais qu'actuellement une association de chercheurs hollandais envisage de stocker des informations sur l'ADN d'une personne sur une carte à puce en vue de permettre la découverte de maladies de son titulaire. C'est un vrai problème d'éthique et de sécurité. S'agissant des drones, vous avez parlé de réponses capacitaires. On n'a pas le droit de tirer sur un objet volant à un mètre du sol. Faut-il modifier la loi pour pouvoir tirer ? Que pensez-vous du laser chinois qui détruit des drones, mentionné dans la presse ?

Mme Hélène Conway-Mouret. – Je vous remercie pour votre présentation. Je souhaite revenir sur le plan Vigipirate et sur sa refonte que vous avez évoquée. Quelles sont les grandes modifications pour le rendre plus efficace et plus accessible ? Par ailleurs, en tant qu'ancienne auditrice de l'IHEDN, je me demande où seront réalisées les 2% d'économies annoncées tant à l'IHEDN qu'à l'INHESJ.

M. Louis Gautier, secrétaire général de la défense et de la sécurité nationale.- Certaines choses ont été modifiées, notamment le contrôle dans les aéroports a été renforcé. Pour Vigipirate, c'est surtout la philosophie qui a changé. On est passé d'un système horizontal qui ne couvrait pas tout le spectre des risques à un système vertical qui est décliné désormais par domaine ministériel et chez les grands opérateurs comme la SNCF, EDF. L'important toutefois, c'est de mieux coordonner les actions, notamment au niveau du département. On sait bien que l'efficacité des dispositifs de contrôles renforcés ne peut être absolue. Cependant, ils sont utiles et dissuasifs, je pense aux grands magasins à la veille des fêtes. Les modes du terrorisme ont changé depuis les années 80. La lisibilité des actes terroristes ne passe plus nécessairement par des actions toujours ciblées, de revendications et un message politique clairs. Notre rôle est de veiller à ce que tous les scénarios soient prévus, que les mesures soient réversibles. L'implication du réseau préfectoral est absolument primordiale car les préfets connaissent bien leur département et la situation de terrain. S'agissant de l'IHEDN et de l'INHESJ, l'économie programmée porte sur la

réduction planifiée de deux emplois équivalents temps plein par an dans chacun de ces établissements, mais leur plafond d'emploi, respectivement de 96 et 75 ETP, est relativement important. Il s'agit d'une rationalisation de tâches et des fonctions. Pour contenir, voire réduire les charges de fonctionnement de ces deux établissements situés sur le même site, je prête une attention à la mutualisation de leurs fonctions supports. Est-il choquant de centraliser l'agence comptable, par exemple ?

M. Yves Pozzo di Borgo. – En me rendant au Conseil de l'Europe récemment, j'ai découvert que celui-ci travaillait sur une règlementation de l'utilisation des drones. Suivez-vous ce texte ? Même s'il n'a pas de valeur normative, cela peut peut-être avoir des conséquences.

M. Alain Gournac. – Ma question porte sur le plan Vigipirate. Ne pensez-vous pas que le citoyen devrait mieux connaître et comprendre ce plan ? Ne serait-il pas encore mieux que le citoyen soit intégré au plan, comme au Japon, même si certaines choses doivent, je le comprends bien, rester secrètes. Tout comme vous, je trouve très bien d'avoir la possibilité de descendre le niveau d'alerte.

M. Louis Gautier, secrétaire général de la défense et de la sécurité nationale. - Vous avez tellement raison M. Gournac. Nous avons déclassifié environ 200 des 300 mesures Vigipirate pour qu'elles soient communicables immédiatement à certains élus et responsables. Le plan Vigipirate est désormais accessible sur le site Internet du SGDSN, que nous allons revoir, et sur le site du service d'information du Gouvernement. D'une façon générale, ces plans de gestion des crises ont vocation à être connus mais il doit y avoir des éléments d'adaptation en fonction des publics visés. La pédagogie est différente selon qu'il s'agit de scolaires ou de sportifs par exemple. Il faut préparer la population à la possible survenue de dangers graves tout en évitant que la communication ait des effets anxiogènes. Les mesures doivent être expliquées. Il y a une éducation à faire. M. Pozzo di Borgo, vous attirez mon attention sur une information que je ne connaissais pas et je vais y regarder de très près.

M. Jean-Pierre Raffarin, président. – Certains membres de la commission reviennent de New York et d'autres d'Asie. Nous faisons le même constat d'une mobilisation autour d'Ebola. Nous sommes surpris de voir que ce sujet a une importance très faible en France, du moins ce sont nos impressions. M. le Secrétaire général, je vous remercie ainsi que votre équipe.

ANNEXE II - LISTE DES PERSONNES ENTENDUES PAR LES RAPPORTEURS

Général de corps d'armée Bernard de Courrèges d'Ustou, directeur de l'Institut des hautes études de défense nationale et de l'Enseignement militaire supérieur et **M. le Préfet Joël Bouchité**, directeur adjoint et secrétaire général de l'Institut des hautes études de défense nationale ;

M. Guillaume Poupard, directeur général de l'ANSSI et **M. Christian Daviot**, conseiller « stratégie » ;

Contre-Amiral Arnaud Coustillière, officier général à la cyberdéfense à l'état-major des armées, ministère de la défense.