N° 166

SÉNAT

SESSION ORDINAIRE DE 2015-2016

Enregistré à la Présidence du Sénat le 19 novembre 2015

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* **2016**, *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, Mmes Nathalie Goulet, 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, MM. Gaëtan Gorce, Alain Gournac, Mme Sylvie Goy-Chavent, MM. Jean-Pierre Grand, Jean-Noël Guérini, Claude Haut, 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, Raymond Vall.

Voir les numéros :

Assemblée nationale (**14**ème législ.) : **3096, 3110 à 3117** et T.A. **602**

Sénat : **163** et **164** à **170** (2015-2016)

SOMMAIRE

LES PRINCIPALES OBSERVATIONS DE VOS RAPPORTEURS POUR AVIS

1. La demande de crédits inscrite dans le projet de loi de finances pour 2016 dans le programme 129 « Coordination du travail gouvernemental » est de 618,4 millions d'euros, soit 47 % des CP prévus pour l'ensemble de la mission « Direction de l'action du gouvernement ».

Au sein de ce programme, les crédits sous examen de vos rapporteurs pour avis correspondent à **l'action 02 « Coordination de la sécurité et de la défense** » dotée de **289,46 millions d'euros** (258,19 en 2015) en autorisations d'engagement et **283,94 millions d'euros** de crédits de paiement en 2016 (290,01 en 2015).

Cette action 2 regroupe les crédits du Secrétariat général de la défense et de la sécurité nationale (SGDSN) et de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) , les subventions pour charges de service public de deux instituts placés sous la tutelle du SGDSN : l'Institut des Hautes études de défense nationale (IHEDN) et l'Institut national des Hautes études de la sécurité et de la justice (INHESJ), la dotation en fonds spéciaux et les crédits de fonctionnement et de rémunération de personnels du Groupement interministériel de contrôle (GIC).

Par rapport à la prévision inscrite en loi de finances initiale pour 2015, la dotation de cette action enregistre une **diminution de 3,2** % en CP (**- 9,3 millions d'euros**). Cette évolution est liée, pour l'essentiel, à une diminution des dépenses d'investissement (- 11,5 millions d'euros). En revanche, la dotation progresse de 10,7 % en autorisations d'engagement (+ 27,9 millions d'euros) ce qui devrait permettre une remontée du niveau des investissements en crédits de paiement dans les prochaines années.

2. L'évolution du budget du SGDSN continue de s'inscrire principalement dans la priorité, portée par l'ANSSI, de **montée en puissance de la politique de sécurité des systèmes d'information et de protection des intérêts nationaux contre la cybercriminalité**, et confirmée par la loi de programmation militaire 2014-2019.

L'ANSSI représente désormais plus de la moitié des effectifs budgétaires et des efforts d'investissement du SGDSN ainsi que 70 % de ses crédits de fonctionnement. Cette proportion augmentera encore avec sa montée en puissance.

2.1. Le plafond d'emplois du SGDSN (hors ANSSI), relevant des orientations du Premier ministre pour les secteurs non prioritaires, subira une diminution d'un emploi par an sur la période 2015-2017.

La poursuite des créations d'emplois au profit de l'ANSSI sur la période triennale 2015-2017 est confirmée. Le plafond d'effectifs de l'ANSSI fixé à 455 ETPT en loi de finances initiale pour 2015 est porté à 507 en 2016. Cette montée en puissance constitue un défi structurel pour l'ANSSI qui doit également pourvoir au *turn over* relativement important de ses agents. Elle doit à la fois recruter en nombre et maintenir le niveau qualitatif de ce recrutement ce qui est compliqué compte tenu de la faiblesse du vivier mais surtout du niveau des rémunérations offertes par

le secteur privé lorsqu'il s'agit de cadres ou de techniciens expérimentés. Le départ d'agents de l'ANSSI peut favoriser l'émergence d'un réseau lorsque les industriels et notamment les prestataires de service de cybersécurité qui embauchent ces personnels sont considérés comme de confiance. Paradoxalement, plus son action de sensibilisation est efficace, plus la concurrence sur le marché du travail est vive.

Vos rapporteurs estiment que face à ces difficultés spécifiques, l'ANSSI doit être soutenue en pérennisant les emplois autorisés mais non pourvus lors de la fixation des plafonds d'emplois en loi de finances, afin de lui permettre de lisser les recrutements et en maintenant une certaine souplesse au niveau des rémunérations susceptibles d'être servies pour des contrats à durée indéterminée lorsque la qualité du recrutement ou de la pérennisation dans l'emploi le justifie.

À plus long terme, une politique active de développement de filières de formation en écoles d'ingénieurs et en universités doit être conduite. La faiblesse du vivier est inquiétante d'autant que de nombreuses administrations de la défense, de l'intérieur, de l'économie et des finances, d'autres services du Premier ministre (comme le GIC) ou soutenus par lui comme la nouvelle CNCTR ou la CNIL recherchent des profils analogues ou voisins, sans parler des entreprises du secteur privé.

2.2. L'ANSSI représente une part importante des crédits hors titre 2. Ses dotations sont passées de 25,3 millions d'euros en loi de finances initiale pour 2009 à 68,8 millions dans le projet de loi de finances pour 2016. Elles progressent en crédits de paiement (1,5 %) comme en autorisations d'engagement (+ 29 %) alors que les crédits des autres postes diminuent.

La réalisation d'un centre d'hébergement de données (data center) sécurisé pour l'ANSSI représente le principal investissement. Un montant de 16,1 millions d'euros en AE et 8,5 millions de CP lui est consacré. Il sera cofinancé avec le ministère de l'intérieur, maître d'ouvrage, et sera livré au plus tard en 2019.

3. Les subventions destinées à l'IHEDN et à l'INHESJ sont prévues à hauteur de 16,8 millions d'euros dans le projet de loi de finances pour 2016 à comparer avec 17,4 millions d'euros en loi de finances initiale pour 2015. Ces opérateurs sont en pleine restructuration, après l'élaboration d'orientations stratégiques, ils vont entrer en phase de négociation d'un contrat de performance avec l'État. L'un des objectifs principaux est la mutualisation des moyens et le développement de synergies entre les deux établissements qui seront désormais tous les deux installés sur le site de l'École militaire.

Vos rapporteurs mesurent la portée de ce rapprochement dont ils estimaient dans leur précédent avis qu'il était cohérent avec le continuum dégagé dès le Livre blanc de 2008 entre la défense et la sécurité nationale, tout en conservant la personnalité propre de chacun des deux établissements. **Ce rapprochement doit être l'un des axes des contrats de performance qui seront présentés et approuvés au premier semestre 2016.**

Ils souhaiteraient que les rapporteurs pour avis puissent avoir communication de ce document avant qu'il soit soumis pour adoption au conseil d'administration.

Il serait souhaitable également que ces contrats pluriannuels qui engagent les établissements sur la conduite de leur stratégie et sur la

modernisation de leur gestion, soient également engageants pour l'État en termes de stabilité des ressources publiques apportées.

4. Les fonds spéciaux s'élèvent à 47,3 millions d'euros. Ils sont attribués aux services de renseignement et au Groupement interministériel de contrôle. Leur montant a été diminué de près de 2,6 millions d'euros en raison de la prise en charge budgétaire de la rémunération de ses personnels, jusqu'à présent rémunérés sur fonds spéciaux, sur le titre 2 d'une nouvelle sous-action « Groupement interministériel de contrôle», ce qui est un facteur de transparence que votre commission salue.

5. Le Groupement interministériel de contrôle (GIC) est un service du Premier ministre chargé des interceptions de sécurité et du recueil des données de connexion. La loi n° 2015-912 du 24 juillet 2015 relative au renseignement prévoit un éventail de techniques de renseignement, dont le processus d'autorisation et de mise en œuvre devra faire l'objet d'une traçabilité et d'une centralisation par le GIC. En vue de répondre à ses nouvelles missions, il devra augmenter les capacités de ses équipements et renforcer ses effectifs.

P**our tenir compte des besoins exprimés, le plafond d'emplois du GIC est établi à 80 ETPT et en conséquence, le titre 2 est doté de crédits à hauteur de 3,9 millions d'euros.** Les personnels contractuels du GIC seront donc, à compter de 2016, rémunérés sur les crédits de la sous-action créée à cet effet.

Enfin, le GIC qui recevait **des crédits de fonctionnement** à hauteur de 300 000 euros, verra ce montant **porté à 500 000 euros en 2016**.

6. – *Sous le bénéfice de ces observations, votre commission des affaires étrangères, de la défense et des forces armées, pour ce qui concerne le programme 129, a donné 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 2016***.**

Mesdames, Messieurs,

L'examen des crédits du programme 129 « Coordination du travail gouvernemental » de la mission « Direction de l'action du Gouvernement », qui relève du Premier ministre, fournit à votre commission 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, placé auprès du Premier ministre, 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 interministériels affectés au renseignement, notamment au travers des fonds spéciaux destinés aux services de renseignement, du suivi des moyens du Groupement interministériel de contrôle (GIC), organe qui, au sein des services du Premier ministre, est chargé de déployer les moyens afin de réaliser les interceptions de sécurité et l'accès aux données de connexion dans les conditions fixées par le code de la sécurité intérieure et de l'Académie du renseignement en charge d'actions de formation.

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. Les crédits sont principalement inscrits à **l'action 2 « Coordination de la sécurité et de la défense »** dotée dans le projet de loi de finances pour 2016 de **289,46 millions d'euros** (258,19 en 2015) en autorisations d'engagement et **283,94 millions d'euros** de crédits de paiement en 2016 (290,01 en 2015).

[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*

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	2016	70 657 605	218 808 719	**289 466 324**
	2015	(64 294 320)	(197 192 881)	**(261 487 201)**
Crédits de paiement	2016	70 657 605	213 282 268	**283 939 873**
	2015	(64 294 320)	(229 007 863)	**(293 302 183)**

En euros.

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

Cette action 2 regroupe notamment :

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

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

- la dotation en fonds spéciaux ;

- les crédits de fonctionnement et de rémunération de personnels du Groupement interministériel de contrôle (GIC).

RÉPARTITION PAR SOUS-ACTIONS DES CRÉDITS DE L'ACTION 2 « COORDINATION DE LA SÉCURITÉ ET DE LA DÉFENSE » DU PROGRAMME 129

	2015		**2016**	
	AE	*CP*	*AE*	*CP*
SGDSN	***211 287 201***	***243 102 183***	***237 716 324***	***232 189 873***
Titre2	64 294 320	64 294 320	70 657 605	70 657 605
Hors titre 2	146 992 881	178 807 863	170 958 719	165 432 268
Fonds spéciaux *	***50 200 000***	***50 200 000***	***47 350 000***	***47 350 000***
GIC			***4 400 000***	***4 400 000***
Titre2			3 900 000	3 900 000
Hors titre 2			500 000	500 000
Total action 2	**261 487 201**	**293 302 183**	**289 466 324**	**283 939 873**

** y compris GIC*
Sources : PLF 2015 et 2016

Pour être complet sur l'environnement défense et sécurité nationale, on y ajoutera les crédits destinés au financement de l'Académie du renseignement inclus dans l'action 1 : « Coordination du travail gouvernemental ». Il faudrait également examiner ceux inscrits au programme 308 de la mission « Direction de l'action du gouvernement » pour la Commission nationale de contrôle des techniques de renseignement.

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

A. LE SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN), OUTIL DE GESTION DES CRISES

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'État 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 conduit également des travaux interministériels d'anticipation et de prévention portant sur des pays susceptibles de connaître une crise ou sur des aspects transversaux concernant des crises en cours ou qui se profilent, pouvant affecter nos intérêts, afin d'émettre des recommandations aux autorités politiques.

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 particulier dans la perspective du prochain sommet de l'OTAN à Varsovie (été 2016). Il coordonne également les travaux du groupe interministériel sur la **dissémination des armements conventionnels**, en vue de renforcer la lutte contre les trafics et d'aider les États d'Afrique francophone 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.

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

(1) La lutte contre la prolifération

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 et la Syrie**.

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 les travaux interministériels d'évaluation et d'encadrement des projets d'exportation des laboratoires de confinement de type P3 et P4.

Le SGDSN assure la coordination de la réponse nationale aux interceptions réalisées dans le cadre de la PSI (*Proliferation Security Initiative*), en propre ou avec le concours de divers partenaires étrangers. La fréquence de ces interceptions ne cesse de croître depuis la mise en œuvre de la PSI. Dix-sept affaires d'interception de biens proliférant ont ainsi été menées dans ce cadre depuis l'été 2014.

(2) La protection du potentiel scientifique et technique

Le SGDSN pilote **la montée en puissance du dispositif de protection du potentiel scientifique et technique de la nation (PPST)**. À ce titre, il reçoit les demandes de création de zones à régime restrictif (*ZRR)*, et autorise la prise des arrêtés de création par les ministères concernés. Les efforts de sensibilisation des opérateurs contribuent à entretenir la dynamique de création de ces zones. À ce jour, 451 ZRR ont été créées.

(3) La sécurité des programmes spatiaux européens

Dans le domaine spatial, le SGDSN assure la synthèse des positions nationales sur les questions de sécurité des programmes européens de navigation par satellite (*GALILEO* et *EGNOS*) et de surveillance de la Terre (*COPERNICUS*). Ainsi, s'agissant du programme *GALILEO,* il traite les questions liées à la sécurité et au service public réglementé (PRS, *Public reglemented service*) et assure pour la France la fonction d'Autorité responsable du PRS. En 2015, les travaux pilotés par le SGDSN ont notamment conduit à finaliser avec nos partenaires européens et avec la Commission européenne les règles à appliquer par les nations utilisatrices du service public réglementé, qu'elles

appartiennent à l'Union européenne, ou qu'il s'agisse d'États tiers (« normes minimales communes »).

(4) Contrôle des images spatiales

Le SGDSN pilote la commission interministérielle des données d'origine spatiale (CIDOS), qui assure le contrôle de diffusion des images spatiales par les opérateurs industriels. En 2015, le SGDSN a également conduit, en liaison avec le SGAE, la coordination interministérielle pour l'élaboration de la position française relative à la proposition de directive européenne sur le contrôle des images spatiales[1].

(5) Le contrôle des exportations et transferts intracommunautaires (matériels de guerre et biens à double usage)

En application de la loi n° 2011-702 du 22 juin 2011, **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).

Bilan de la CIEEMG (2014-2015)

Depuis l'introduction de la procédure simplifiée de « licence unique » le 4 juin 2014 et jusqu'au 31 août 2015, la CIEEMG s'est réunie 13 fois en session plénière. Sur la période, la CIEEMG a examiné 8 240 dossiers correspondant à 7 209 dépôts de nouvelles « demandes de licences » et 1 031 demandes de « modification de licences » déjà accordées.

Environ 95 % des demandes (soit 7 866 dossiers) ont fait l'objet d'un traitement en procédure « continue »[2] avec avis favorable. La CIEEMG réunie en session plénière a examiné 374 dossiers et prononcé 262 avis favorables et 112 avis défavorables[3].

Le SGDSN a actualisé en mars 2015 les « directives de haut niveau », qui servent de cadre méthodologique aux décisions proposées à l'exécutif par la CIEEMG et piloté différents travaux interministériels d'adaptation de la réglementation en matière de contrôle d'armements[4]. Il apporte son

---

[1] *Ces travaux ont conduit, en liaison avec nos principaux partenaires européens, à l'abandon de cette proposition de directive qui était contraire aux principes de la loi n° 2008-518 du 3 juin 2008 relative aux opérations spatiales.*

[2] *Demandes traitées complètement de manière dématérialisée dans le système d'information* SIGALE.

[3] *Les dossiers les plus sensibles ou pour lesquels un avis défavorable est émis sont systématiquement examinés en réunion plénière.*

[4] *Décret n°2015-837 du 8 juillet 2015 portant réforme de la réglementation relative aux armes et matériels de guerre et arrêté du 8 juillet 2015 relatif aux dérogations à l'obligation d'obtention d'une autorisation d'importation de matériels de guerre, armes, éléments d'arme, munitions ou éléments de munition. Arrêté de classement du 16 mars 2015 modifiant l'arrêté du 27 juin 2012.*

expertise à la commission interministérielle des biens à double usage (CIBDU) pour l'instruction des dossiers sensibles.

Au niveau européen, il a coordonné les travaux de publication de deux nouvelles licences générales de transfert[1] encadrant, d'une part, les échanges intracommunautaires technologiques et, d'autre part, les transferts liés au programme *ARIANE 6*. Il participe, en outre, aux travaux internationaux sur les matériels de guerre[2] et sur les biens à double usage[3].

C'est aussi à ce titre que le SGDSN a été amené à suivre, en 2015, les dossiers industriels sensibles comme la sortie du contrat de vente à la Russie de deux bâtiments de projection et de commandement et le projet de rapprochement des groupes industriels, allemand et français, de l'armement terrestre, KMV et NEXTER.

2. Le SGDSN acteur de la politique de sécurité nationale

Les menaces et les risques susceptibles d'affecter la vie de la Nation ainsi que les réponses que les pouvoirs publics doivent y apporter font l'objet de la stratégie de sécurité nationale. De nombreux types de menaces (terrorisme, prolifération des armements et des technologies, cyber-menace, atteinte au potentiel scientifique et technique) et de risques (naturels, industriels, sanitaires et technologiques) se sont développés qui peuvent affecter gravement le fonctionnement de la Nation, en raison des fortes interdépendances entre secteurs d'activités et entre acteurs nationaux et internationaux.

Sur proposition du SGDSN, le Premier ministre a signé, le 11 juin 2015, la nouvelle directive générale interministérielle relative à la planification de défense et de sécurité nationale[4], qui couvre l'ensemble des travaux destinés à préparer les actions à conduire en situation de crise.

Le nouveau dispositif national de planification intègre, dans une perspective plus européenne et internationale, le rôle majeur des acteurs non étatiques dans la gestion des crises, la place des armées dans la continuité

---

[1] *Arrêtés du 14 novembre 2014 et du 28 juillet 2015.*

[2] *Il anime le sous-comité de l'accord-cadre* LoI, *chargé notamment de la simplification des procédures applicables aux transferts entre les six pays membres. Il a notamment permis l'adoption, fin 2014, d'un* papier de position commune *avec des recommandations servant notamment de base aux travaux que conduit la Commission européenne pour l'évaluation de la directive sur les transferts intracommunautaires des produits liés à la défense (rapport prévu mi-2016).*

[3] *En vue des négociations dans les régimes internationaux correspondants (Arrangement de WASSENAAR, Groupe Australie, Missile Technology Control Regime – MTCR, Nuclear Suppliers Group – NSG) ou dans le cadre des partenariats internationaux dans les domaines sensibles, le SGDSN participe à l'établissement de la position technique française.*

[4] http://circulaire.legifrance.gouv.fr/pdf/2015/06/cir_39748.pdf *Cette directive, qui remplace celle de 2001, abroge également plusieurs documents anciens devenus inutiles ou obsolètes.*

des activités de la Nation, les effets de la décentralisation et des réformes de l'organisation territoriale de l'État ainsi que la mise en place d'une nouvelle organisation gouvernementale de crise.

C'est dans ce cadre que se sont poursuivis les travaux de rénovation des plans gouvernementaux.

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

Publié en janvier 2014, **le nouveau plan VIGIPIRATE**[1] fait l'objet d'un processus d'évaluation après un an de mise en œuvre et dans le contexte *post* attentats de janvier 2015.

Au cours de son audition, M. Louis Gautier, Secrétaire général de la défense et de la sécurité nationale, a indiqué que des propositions seront faites au gouvernement sur le plan Vigipirate à la fin du mois de novembre. « *Les retours d'expérience à la fin de l'année 2015 montrent une inadaptation du dispositif. La difficulté vient de la définition des postures. Il n'y a pas de lien entre le plan Vigipirate et la doctrine des armées et notamment le contrat emploi-protection. Le dispositif était prévu pour inclure 1 500 militaires sur le territoire puis 3 000 militaires dans la posture dite « alerte attentat » mais n'envisageait pas le déclenchement du contrat emploi protection des armées. Dans la doctrine des armées, le contrat emploi protection est d'abord prévu pour faire face aux catastrophes. Il envisage la mobilisation massive des capacités militaires mais pendant une durée limitée, par exemple pour faire face aux effets d'une tempête ou d'un accident industriel. Aujourd'hui, il apparaît nécessaire, pour permettre au plan Vigipirate de s'étaler dans la durée, de recréer un lien entre le plan et le contrat emploi protection qui permet de mobiliser désormais jusqu'à 7 000 hommes dans la durée. (…)*

« Cette posture de crise continue d'être appliquée parce qu'elle permettait au départ de mobiliser les effectifs nécessaires mais alors même qu'elle prévoit des options juridiques qui ne peuvent pas être appliquées dans la durée. Elle doit être réservée aux périodes où une menace grave et imminente est décelée ou lorsque l'on recherche des terroristes en fuite par exemple. Il est donc nécessaire de redéfinir une posture d'urgence autour d'une posture alerte attentat qui resterait limitée dans le temps. »

« Enfin, il faut pouvoir territorialiser le plan Vigipirate. Jusqu'ici la logique appliquée envisageait le déploiement des militaires dans le cadre du contrat de protection des armées sous la forme d'une projection intérieure de force à l'instar de la projection extérieure. Mettre en œuvre un déploiement pérenne des forces implique une territorialisation de ce plan. »

Le SGDSN a achevé, à l'automne 2014, la révision du plan PIRATAIR-INTRUSAIR (réponse à des actes illicites mettant en jeu la sûreté aérienne ou la souveraineté aérienne) puis a engagé, en 2015, en lien avec l'*Agence nationale*

[1] http://www.sgdsn.gouv.fr/IMG/pdf/Partie_publique_du_plan_Vigipirate_2014.pdf

de la sécurité des systèmes d'information (ANSSI), la rénovation du plan PIRANET (réponse à des attaques sur les systèmes d'information). La révision du plan PIRATE-MER (réponse à des attaques maritimes) sera ultérieurement engagée, en lien avec le secrétariat général de la mer.

Le SGDSN a également coordonné les travaux interministériels d'élaboration du nouveau plan de prévention et de lutte contre la maladie à virus Ebola. Ce plan, publié le 24 novembre 2014, vise, d'une part, à organiser la réponse à des cas qui pourraient être importés sur le territoire national et, d'autre part, à assurer la prise en charge des ressortissants français ou binationaux qui pourraient être atteints dans les pays où sévit l'épidémie.

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

L'État doit organiser et mettre en œuvre des capacités civiles et militaires pour faire face aux multiples risques et menaces qui peuvent affecter le pays. **Le *contrat général interministériel (CGI)* répond à cette exigence en fixant, pour les cinq 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. Il est établi dans une logique 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. Il comprend une partie générale et deux volets dédiés à la sécurité des systèmes d'information et à la réponse aux menaces NRBC.

Le CGI a été diffusé en février 2015 sous forme d'une instruction générale interministérielle signée par le Premier ministre et les ministres concernés. D'après les réponses fournies par le Gouvernement au questionnaire écrit de vos rapporteurs, la déclinaison territoriale de cette démarche capacitaire a été lancée sous la responsabilité du ministère de l'intérieur. Elle associera plus étroitement qu'aujourd'hui l'ensemble des acteurs territoriaux de la préparation et de la gestion des crises, en particulier les collectivités territoriales et opérateurs économiques, et assurera une parfaite cohérence entre planification gouvernementale et planification locale.

S'agissant de la capacité de **veille et d'alerte** sur les différentes crises au profit des hautes autorités de l'État, le SGDSN est un acteur essentiel de la chaîne d'alerte gouvernementale, dispositif qui s'appuie notamment sur son *Bureau de veille et d'alerte* (BVA), qui coordonne étroitement ses actions avec les centres opérationnels des ministères, vingt-quatre heures sur vingt-quatre. Cette chaîne d'alerte gouvernementale a été systématiquement mise en œuvre à l'occasion des différentes crises survenues en 2015, en particulier

lors des attentats commis à Paris, en janvier dernier et tout récemment encore lors des attentats du 13 novembre.

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

Conformément aux recommandations du *Livre blanc sur la défense et la sécurité nationale*[1], et afin de permettre à l'État et aux *opérateurs d'importance vitale* (OIV) de pouvoir s'appuyer sur des industriels capables de répondre rapidement et au meilleur coût à leurs besoins en solutions de sécurité, le SGDSN a conduit les travaux visant à structurer les industries françaises dans le domaine de la sécurité. Le Premier ministre a installé, fin 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 de la recherche académique française.

Les activités du CoFIS

Le CoFIS promeut la compétitivité de la filière et s'articule ainsi pleinement avec les plans de la Nouvelle France Industrielle et la stratégie nationale de recherche. Il porte sur un secteur sensible devant sur le plan stratégique garantir notre autonomie dans les secteurs les plus critiques tout en assurant le respect des libertés individuelles, qui justifie son pilotage par le Premier ministre.

La filière industrielle de sécurité a produit, depuis sa mise en place, une expression des besoins publics et privés en matière de sécurité. Ces priorités seront soutenues dans la conquête de marchés à l'export, en particulier au bénéfice des PME. Elles seront portées au sein d'une stratégie de recherche et d'innovation avec le lancement de démonstrateurs technologiques (radiocommunications professionnelles du futur, protection de grands événements) et grâce au financement de projets sur des technologies critiques.

Le SGDSN continuera ainsi à participer au financement des projets de sécurité et de cybersécurité *via* l'*agence nationale de la recherche* (ANR) et le *fonds unique interministériel* (FUI)[2], et continuera « *à financer en propre le développement de*

[1] *Le Livre blanc de 2013 s'inspirait des recommandations de votre commission qui avait mis en lumière, dans son rapport d'information sur la cyberdéfense de juillet 2012, la nécessité de consolider une filière industrielle française de la sécurité informatique et de 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'État et le secteur privé (priorité n°7).* « La cyberdéfense : un enjeu mondial, une priorité nationale » *Rapport d'information de M. Jean-Marie Bockel, n° 681 (2011-2012) - 18 juillet 2012* http://www.senat.fr/notice-rapport/2011/r11-681-notice.html

[2] *Voir infra p.47*

nouvelles solutions de lutte contre les risques nucléaires, radiologiques, biologiques, chimiques et explosifs. Enfin, le SGDSN poursuivra son action de promotion des intérêts français dans le cadre du programme européen Horizon 2020 ».

Source : SGDSN - Réponses au questionnaire parlementaire

d) Le renforcement des politiques de protection contre les menaces et risques majeurs

(1) Le mandat relatif à l'engagement des armées sur le territoire national

À la suite des attentats de janvier 2015, le Président de la République a décidé, conformément aux missions de protection dévolues aux armées par la loi de programmation militaire 2014-2019 adoptée en décembre 2013, de déployer massivement des militaires pour protéger la population et certains sites sur le territoire national.

Les diverses implications de l'opération « *SENTINELLE* », exceptionnelle dans son ampleur et dans sa durée, doivent être évaluées précisément car le nouveau contrat stratégique mis en place par la loi n° 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense prévoit la capacité de déployer 7 000 hommes dans la durée sur le territoire.

Les conséquences de ce nouveau contrat stratégique doivent être tirées sur le rôle de l'armée par rapport aux forces de sécurité intérieure et de sécurité civile, sur la chaîne de commandement, sur le cadre juridique de l'intervention des militaires, sur la doctrine d'emploi, sur la préparation opérationnelle et la formation ou encore sur le type de sites à protéger et les modalités de cette protection.

En réponse aux décisions prises par le Président de la République lors du conseil de défense et de sécurité nationale du 29 avril 2015, **le Premier ministre a demandé au SGDSN d'identifier, avec l'ensemble des acteurs concernés, les adaptations nécessaires pour garantir la disponibilité, la capacité d'action et l'efficacité des forces militaires engagées sur le territoire national.**

Fondés sur le retour d'expérience des mois écoulés depuis le déclenchement de la mission « *SENTINELLE* », ces travaux doivent permettre d'identifier des évolutions pragmatiques à court et moyen termes. Les modes d'action, le partage des prérogatives et des responsabilités entre forces militaires et de sécurité intérieure, ainsi que la coordination militaire, seront notamment étudiées.

Pour autant, **cette réflexion doit également s'inscrire dans une remise en perspective plus générale du rôle spécifique des armées dans la protection du territoire national**. Dans ce cadre, l'évolution du cadre juridique actuel doit être aussi étudiée.

Ces travaux, dont les conclusions seront rendues en décembre 2015, précéderont **la remise, avant le 31 janvier 2016, d'un rapport du Gouvernement au Parlement sur les conditions d'emploi des armées sur le territoire national** selon les dispositions introduites par votre Commission dans la loi n° 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense[1]. Ce rapport fera l'objet d'un débat au Parlement.

(2) La consolidation des dispositifs interministériels de prévention et de protection

Le SGDSN poursuit **le renforcement de la politique de *sécurité des activités d'importance vitale* (SAIV).** Ainsi, la révision des *directives nationales de sécurité* (DNS) vise à élargir leur conception à une approche « tous risques », incluant la planification de la continuité des activités face à un large éventail de risques, et à renforcer la sécurité des systèmes d'information, en étroite collaboration avec l'ANSSI. Six DNS rénovées ont ainsi été approuvées (« communications électroniques et internet », « électricité », « gaz », « hydrocarbures » « produits de santé » et « transport aérien ») et la révision de onze autres est engagée.

Pour contribuer à la résilience du pays, le SGDSN a mandaté le *haut fonctionnaire de défense et de sécurité* des ministères économiques et financiers pour développer une offre française concurrentielle de certification des plans de continuité d'activité en raison des enjeux de compétitivité et de sécurité économique associés. Par ailleurs, une action a été engagée pour identifier les besoins ministériels en spécialistes de la sécurité des systèmes d'information et promouvoir le développement des métiers et de la formation pour y répondre. Le SGDSN a continué à accompagner les ministères dans l'élaboration de leurs plans de continuité d'activité respectifs, notamment face au risque de crue majeure de la Seine.

(3) La protection des installations et des sites sensibles

Concernant **la protection physique des installations nucléaires**, le SGDSN a poursuivi la mise en œuvre des conclusions des travaux interministériels menés depuis 2014. Ainsi, après la modification de la partie législative du code général des collectivités territoriales qui permet aux préfets de département de réglementer la circulation et le stationnement aux abords des installations nucléaires, la loi du 2 juin 2015 relative au renforcement de la protection des installations civiles abritant des matières nucléaires a permis de créer le délit d'intrusion dans une installation nucléaire. Les travaux se poursuivent sur le décret d'application de cette loi

[1] *Article 7 :* « Le Gouvernement remet, avant le 31 janvier 2016, un rapport au Parlement sur les conditions d'emploi des forces armées lorsqu'elles interviennent sur le territoire national pour protéger la population. Ce rapport fait l'objet d'un débat ».

ainsi que sur les capacités des services internes de sécurité et sur les dispositifs de protection physique des opérateurs nucléaires.

Dans l'éventualité d'un incident ou d'un accident sur une centrale nucléaire, le SGDSN a coordonné l'élaboration d'une convention d'assistance de l'État à EDF pour la projection, par vecteur aérien, d'une équipe de reconnaissance de la *force d'action rapide nucléaire* (FARN) de l'opérateur en cas de situation d'urgence sur une installation. Elle a été signée le 6 novembre 2014 par les parties prenantes.

Dans le cadre du plan d'actions lancé par le Gouvernement pour renforcer la sécurité des sites industriels sensibles, le cabinet du Premier ministre a donné mandat au SGDSN pour réfléchir à une meilleure prise en compte de la menace malveillante et terroriste dans la sécurité des installations classées pour la protection de l'environnement, et notamment l'articulation de cette réglementation avec le dispositif de sécurité des activités d'importance vitale.

À la suite des attentats qui ont visé deux sites Seveso à l'été 2015, le SGDSN a édité, en août 2015, en partenariat avec les ministères concernés, **un guide** conçu par *l'institut national de l'environnement industriel et des risques* (INERIS), **diffusé en premier lieu aux exploitants des 1 200 installations industrielles Seveso, pour leur permettre de réaliser l'auto-évaluation de la vulnérabilité de leur site** face aux actes de malveillance et de terrorisme.

(4) Le développement de l'analyse de risque au profit de la capacité d'anticipation de l'État

Cette démarche, engagée en 2012 en lien étroit avec le *coordonnateur national du renseignement* (CNR), a permis de mieux prendre en compte l'évaluation de la menace dans le dispositif du nouveau plan VIGIPIRATE et de mieux délimiter les capacités critiques dans le cadre du « contrat général interministériel ».

Dans le cadre de la prise en compte de la dimension internationale des menaces, le SGDSN a poursuivi, en lien avec le CNR et les ministères concernés, ses coopérations dans le domaine de la prévention et de la lutte contre le terrorisme, en particulier avec le Royaume-Uni, les États-Unis et l'Allemagne.

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

Dans le domaine NRBC, l'analyse des risques s'est appuyée sur l'élaboration, en 2014, d'une dizaine de scénarios de référence qui servent dorénavant de base au perfectionnement du dispositif de réponse dans le cadre du comité stratégique NRBCE. En ce domaine, **un point de vigilance**

particulier doit être le maintien des stocks de produits utilisés dans la lutte contre les risques NRBC et leur renouvellement, car ces produits se périment.

Dans le secteur du transport aérien, avec l'appui du pôle d'analyse du risque pour l'aviation civile de la *direction générale de l'aviation civile*, le SGDSN a poursuivi 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 »). Le programme d'évaluation des escales sensibles sera ainsi poursuivi avec une attention particulière sur la mise en œuvre du nouveau cadre législatif en vigueur (article 23 de la loi du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme), tandis que le programme de lutte contre la menace MANPADS sera étendu aux plates-formes aéroportuaires nationales.

S'agissant de la menace représentée par l'usage malveillant des drones de loisir, le SGDSN a coordonné les études interministérielles lancées en novembre 2014 à la suite des survols illicites de sites sensibles. Elles ont permis de caractériser la menace, de proposer les adaptations législatives et réglementaires pour mieux encadrer l'usage des drones et de travailler sur les réponses capacitaires de détection et de neutralisation de ce type d'aéronefs. **L'ensemble des travaux est détaillé dans le rapport du Gouvernement au Parlement déposé fin octobre 2015**[1].

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

La professionnalisation des acteurs de la gestion des crises majeures passe par **l'organisation, chaque année, de trois à quatre exercices majeurs afin de tester la capacité de l'État à mettre en œuvre une réponse politique et stratégique face à une crise**. Ces exercices mobilisent systématiquement le cabinet du Premier ministre et les directions centrales des ministères à travers notamment l'activation de la *cellule interministérielle de crise*.

En 2014, trois exercices ont été dédiés à la thématique terroriste et ont permis l'évaluation des plans VIGIPIRATE et PIRATAIR-INTRUSAIR rénovés, ainsi que le renforcement de la coordination politico-stratégique entre la France et le Royaume-Uni.

En 2015, le SGDSN a retenu trois thématiques différentes : la simulation d'une rupture d'approvisionnement de gaz en France, l'organisation d'un grand événement sportif dans un contexte de menace terroriste élevée et la gestion d'une d'attaque cyber visant le transport d'électricité. Par ailleurs, un exercice franco-américain construit sur un scénario de terrorisme biologique s'est déroulé à Paris en janvier 2015.

---

[1] *« L'essor des drones aériens civils en France : enjeux et réponses possibles de l'État »* http://www.sgdsn.gouv.fr/IMG/pdf/151016_Rapport_du_gouvernement_au_parlement_sur_les_drones.pdf

e) L'amélioration de la protection du secret de la défense nationale

Le développement des inspections relatives au respect des règles de protection des informations classées Très Secret, dont le SGDSN a la pleine responsabilité, a été poursuivi. Plus de 20 inspections ont été menées en 2014 sur des emprises de l'État et de certaines entreprises.

De nouveaux accords généraux de sécurité (AGS) ont été négociés ou renégociés avec des États étrangers.

Plus fondamentalement, une révision en profondeur de l'instruction générale interministérielle (IGI) n° 1300 du 30 novembre 2011 qui organise en France la protection du secret de la défense nationale est engagée. Des consultations interministérielles sont conduites pour mieux prendre en compte la dématérialisation des données dans la réglementation relative aux informations classifiées et mieux mettre en adéquation notre droit et nos pratiques avec ceux de nos principaux partenaires.

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

Le secrétaire général de la défense et de la sécurité nationale a aux termes du 7° de l'article R.132-3 du code de la défense, la mission de proposer au Premier ministre et de mettre en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information. Il dispose à cette fin d'un service à compétence nationale « Agence nationale de la sécurité des systèmes d'information (ANSSI) » (décret n°2009-834 du 7 juillet 2009).

Le positionnement de l'Agence auprès du Secrétaire général de la défense et de la sécurité nationale, en sa qualité de conseiller du Premier ministre en matière de défense et de sécurité, est important compte tenu des enjeux. Il permet de les faire valoir dans les instances de décision au plus haut niveau de l'État. Il a, en revanche, pour inconvénient, d'inscrire l'ANSSI dans un circuit de décision administrative et budgétaire parfois contraignant auquel le SGDSN s'efforce d'apporter en gestion un peu plus de souplesse.

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.

De fait, **l'étendue de la menace ne cesse de s'accroître**. La France est classée au 14ème rang mondial des pays où la cybercriminalité est la plus active[1].

L'augmentation exponentielle des cyberattaques

D'après le 20ème rapport de la société américaine de sécurité informatique Symantec portant sur l'année 2014, les cyber-attaquants ont opéré un changement de tactique en s'infiltrant dans les réseaux et en échappant à toute détection par le détournement de l'infrastructure des grandes entreprises et en l'utilisant contre elles. Ils piègent notamment les entreprises en les faisant s'auto-infecter via des chevaux de Troie lors de mises à jour de logiciels standard. Ils attendent ensuite patiemment que leurs cibles téléchargent ces mises à jour infectées, leur donnant ainsi libre accès au réseau de l'entreprise. 2014 aura par ailleurs été une année record pour les vulnérabilités zero-day, avec une moyenne de 59 jours pour que les éditeurs de logiciels créent et déploient des correctifs.

Les attaques touchant les entreprises sont en outre toujours plus ciblées et plus précises. Elles ont eu recours à 20 % d'e-mails en moins pour parvenir à leurs fins et incorporé plus de logiciels malveillants par téléchargement et autres exploits en ligne. On a pu également observer que les attaquants utilisent des comptes de messagerie volés à une victime d'une entreprise afin d'en harponner d'autres au bout de la chaîne, profitent des outils et procédures de gestion des entreprises pour déplacer les IP volées au sein du réseau d'entreprise avant de les en extraire, ou encore conçoivent des logiciels d'attaque personnalisés.

Si les attaques sont toujours plus ciblées, la cybercriminalité générale ne décroit pas, bien au contraire : 317 millions de nouveaux programmes malveillants ont été créés en 2014, soit près de 1 million par jour. L'e-mail reste un vecteur d'attaque important pour les cybercriminels, mais ces derniers continuent d'expérimenter de nouvelles méthodes d'attaque sur les périphériques mobiles et les réseaux sociaux afin d'atteindre plus de personnes, en faisant des efforts moindres. Ces techniques « faciles » continuent de rapporter, mais certains cybercriminels se tournent vers des méthodes d'attaque plus lucratives et agressives comme le *ransomware*, qui bloque littéralement le terminal en otage contre le versement d'une rançon. L'an dernier, ce type de programme malveillant a augmenté de 113 % et sa variante « *cryptolocker* », qui chiffre les données, a fait 45 fois plus de victimes qu'en 2013.

La France progresse à nouveau cette année d'un rang et passe donc au 14ème rang mondial et au 6ème rang européen des pays où la cybercriminalité est la plus active, les États-Unis, la Chine et l'Inde conservant le haut du classement. Si l'on note une baisse du spam et des attaques web, on voit également qu'elle a subi encore plus d'attaques réseaux et par *phishing* en 2014 et 2013, occupant respectivement la 6ème et 4ème place mondiale. Autre fait distinctif français : si les grandes entreprises sont particulièrement concernées (59 %) par les attaques ciblées, il en est de même pour les PME (35,6 %) et ce, de façon différente des statistiques mondiales. L'exception culturelle française en matière de cybercriminalité concerne d'une part les arnaques sur les réseaux sociaux : la France se classe au 5ème rang mondial et 2ème rang européen (derrière le Royaume-Uni et devant l'Allemagne), d'autre part l'extorsion numérique, avec les *ransomware* (4ème rang européen et 6ème rang mondial) dont les *cryptolockers* représentent désormais 9% dans le pays.

[1] *20 ème Rapport de la société américaine de sécurité informatique Symantec avril 2015*

Ces informations sont corroborées par une étude récente publiée par PricewaterhouseCoopers qui indique que le nombre de cyberattaques en 2015 a augmenté de 51 % en France. Les entreprises françaises subiraient en moyenne 21 incidents par jour.

Sources : Laurent Heslaut ***http://www.observatoire-fic.com/conclusion-du-rapport-annuel-de-symantec-sur-les-menaces-de-securite-sur-internet/***

Sophy Caulier « Menaces tous azimuts sur le bigdata » *Le Monde 10 novembre 2015*

L'attaque puissante menée contre la chaîne de télévision francophone TV5Monde en avril 2015 qui a conduit à l'interruption du service sur l'ensemble des réseaux de diffusion hertziens, câblés et numériques constitue un exemple visible des capacités de destruction des cyberattaques. Elle ne représente toutefois qu'une partie des attaques et des dommages dont sont victimes les administrations, entreprises et particuliers. Les victimes préfèrent souvent s'abstenir de communiquer sur ces attaques, leur révélation pouvant entraîner des impacts collatéraux déstabilisateurs.

TV5Monde : une attaque majeure et un exemple d'intervention de l'ANSSI

Le 8 avril 2015, la chaîne internationale TV5Monde a été victime d'une cyberattaque majeure conduisant à un effondrement de son système d'information l'empêchant de diffuser les douze chaînes de télévision qu'elle produit.

Bien qu'il ne s'agisse pas d'un opérateur d'importance vitale, l'ANSSI est intervenu immédiatement compte tenu de l'importance de l'attaque. Pour son directeur général « *Dans le domaine de la réaction, TV5Monde fournit un bon exemple des niveaux d'intervention mis en œuvre par l'ANSSI qui est le seul intervenant français à pouvoir le faire à ce niveau. Dès l'attaque détectée, nous avons pu projeter des équipes dans les premières heures pour conserver les traces pour les analyses, un peu comme sur une scène de crime, ce qui est une opération compliquée. Il s'agit ensuite de relancer le service. Nous avons pu dans l'exemple de* TV5Monde *rétablir un service, certes dégradé mais visible en moins de 18 heures, ce qui était indispensable pour une chaîne de télévision internationale. Enfin, nous avons accompagné ce média dans la reconstruction d'un réseau solide avec un niveau de sécurité élevé. Notre action est associée au développement d'une capacité de détection efficace, qui nous permet de réagir très rapidement* »[1].

Selon les dirigeants de *TV5Monde,* le préjudice économique s'élève à plusieurs millions d'euros : restauration du système d'information, y compris le remplacement de matériels corrompus, frais de personnels supplémentaires nécessaires pour faire fonctionner l'entreprise sans ses automates de production et de diffusion, pertes de ressources publicitaires et préjudices d'image auprès des téléspectateurs et des annonceurs. En outre, la société devra investir dans un dispositif de protection pour rendre son système d'information plus robuste et mettre en place une supervision afin de détecter sans délai d'éventuelles nouvelles intrusions.

[1] http://www.senat.fr/compte-rendu-commissions/20151012/etr.html#toc4

Interrogé sur la fréquence des attaques, le directeur général de l'ANSSI, M. Guillaume Poupard, indique que « *si l'on se focalise sur les attaques majeures touchant une administration ou un grand industriel à l'image de ce qu'a subi TV5Monde, en début d'année, avec un véritable impact en termes de fonctionnement de l'entreprise ou de compromission d'information, c'est de l'ordre d'une attaque tous les quinze jours* »[1].

Le 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. 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

(1) Des dispositions législatives ont été introduites par 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* ».

Les trois principales dispositions adoptées

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'État, 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'État 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.

[1] *Le Monde 10 novembre 2015*

L'article 22 (articles L. 1332-6-1[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 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'État, 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 progressive avec 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.

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'État désignés par le Premier ministre, **un arrêté du Premier ministre[2] établit la liste restreinte des services de l'État autorisés à bénéficier de cette disposition.**

Les décrets n° 2015-349, 2015-350 et 2015-351 du 27 mars 2015 respectivement relatifs à l'habilitation et à l'assermentation des agents de l'ANSSI, à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale et à la sécurité des systèmes d'information des opérateurs d'importance vitale (OIV) **ont constitué la première étape de la publication des textes d'application**

Parallèlement, dans la cadre de la mise en œuvre de l'article 22 de la loi, **une concertation avec les OIV, par secteur d'activité d'importance vitale et par famille des métiers, a été engagée début 2015** au travers de dix-

[1] *Ces dispositions ont été précisées par des dispositions de l'article 27 de la loi n° 2015-917 du 28 juillet 2015 actualisant la programmation militaire pour les années 2015 à 2019 et portant diverses dispositions concernant la défense*

[2] *Arrêté du 17 juillet 2015 déterminant les services de l'État mentionnés au second alinéa de l'article L. 2321-2 du code de la défense*

huit groupes de travail destinés à étudier la liste des types de systèmes d'information concernés, les mesures techniques à appliquer et leur délai de mise en œuvre. **Les premiers arrêtés** issus de ces travaux, éventuellement protégés par une mention de classification du secret de la défense nationale, **devraient être publiés avant la fin de l'année**.

(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'État, **fixant les règles de protection des systèmes d'information des différents départements ministériels**[1]. Ce document de 40 pages, préparé par l'ANSSI, qui fixe les contours d'une « *Politique de sécurité des systèmes d'information de l'État* » (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.

Un premier bilan de la mise en œuvre de cette politique a été communiqué au Premier ministre et l'ANSSI envisage d'actualiser de PSSIE en fonction de ces résultats et des retours d'expérience issus des travaux ministériels.

La sécurité des systèmes d'information devenant un enjeu essentiel et l'ANSSI représentant plus de la moitié des effectifs budgétaires et des moyens gérés par le SGDSN, il est apparu important d'introduire dans les objectifs et indicateurs de performance du programme 129 un indicateur lié à la sécurité des systèmes d'information de l'État.

Cet indicateur recouvre deux objectifs :

- améliorer la maturité globale des différents départements ministériels en matière de SSI ;
- mener à bien des projets interministériels structurants prévus par le Livre blanc sur la défense et la sécurité nationale de juin 2008 qui ont contribué à justifier la création de l'ANSSI.

[1] *n° 5725/SG du 17 juillet 2014.*

INDICATEUR 6.1

Niveau de sécurité des systèmes d'information de l'État

(du point de vue de l'usager)

	Unité	2013 Réalisation	2014 Réalisation	2015 Prévision PAP 2015	2015 Prévision actualisée	2016 Prévision	2017 Cible
Maturité globale en sécurité des systèmes d'information de l'État	note de 0 à 5	3,10	3,3	3,5	2,2	2,4	2,7
Niveau d'avancement des grands projets interministériels en matière de sécurité des systèmes d'information	%	86	80	85	83	87	89

Précisions méthodologiques

Sous-indicateur « Maturité globale en sécurité des systèmes d'information de l'État »

Source des données : les données sont fournies par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Les données de base sont les niveaux de maturité effectifs (réels) des départements ministériels et les niveaux adéquats à atteindre pour chaque département ministériel.

Modalités de calcul : cet indicateur se présente sous la forme d'une note de 0 à 5, où 5 est l'optimum.

Chaque département ministériel rend périodiquement des comptes à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) sur la conformité de ses systèmes d'information vis-à-vis des règles et objectifs de la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE). Un indicateur synthétique ministériel, entre 0 et 5, est calculé à partir de ces données. Les valeurs transmises par les départements ministériels sont réexaminées en fonction des relevés ponctuels effectués par l'ANSSI, notamment lors des inspections qui les touchent périodiquement.

Une pondération est ensuite apportée aux différentes notes des ministères, afin de tenir compte de l'importance de la sécurité des systèmes d'information, qui diffère d'un ministère à l'autre.

Sous-indicateur « Niveau d'avancement des grands projets interministériels en matière de sécurité des systèmes d'information »

Source des données : les données sont fournies par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Modalités de calcul : la valeur de ce sous-indicateur de politique transversale SSI est obtenue par moyenne de trois indicateurs :

- le taux de connexion des passerelles des organismes de l'État au centre gouvernemental de détection des attaques informatiques ;
- le taux de déploiement des systèmes d'information sécurisés (notamment le réseau téléphonique sécurisé Rimbaud, avec son nouveau terminal TEOREM de cryptophonie de nouvelle génération, et l'intranet gouvernemental (ISIS) par rapport à l'objectif cible ;
- le pourcentage de satisfaction du catalogue objectif des produits de sécurité labélisés par l'ANSSI.

L'ANSSI a souhaité faire évoluer la méthodologie relative à la mesure de la maturité globale en sécurité des systèmes d'information de l'État. Le mode de calcul du premier sous-indicateur a en conséquence évolué en 2015 afin de reposer sur une méthode de calcul plus robuste et moins subjective. Il s'appuie désormais sur un référentiel partagé, à savoir la Politique de sécurité des systèmes d'information de l'État (PSSIE) validée par le Premier ministre pour lequel la mise en conformité des systèmes d'information des ministères fait l'objet d'efforts d'accompagnement spécifiques de la part de l'ANSSI. Ce nouveau mode de calcul ne permet pas

de comparer les prévisions et la cible avec les valeurs des années précédentes.

S'agissant du second sous-indicateur, la prévision actualisée pour l'année 2015 est à un niveau légèrement inférieur à celui prévu initialement en raison du retard d'un an dans le programme de réalisation d'un équipement de sécurité de niveau gouvernemental. Ce glissement limité est sans conséquence sur l'atteinte de la cible 2017.

c) La mise en place d'une stratégie nationale pour la sécurité numérique

Le Premier ministre a présenté, le 18 juin 2015, la stratégie numérique du Gouvernement. Le chapitre « *Egalité des droits : la confiance, socle de la société numérique* » annonce la mise en place courant 2016 d'un dispositif d'assistance aux victimes d'actes de cybermalveillance. L'élaboration de ce dispositif et sa mise en place sont une priorité de l'ANSSI qui travaille en étroite collaboration avec le ministère de l'intérieur.

En outre l'ANSSI a engagé en juin 2014 **un travail interministériel d'élaboration d'une stratégie nationale de sécurité du numérique qui a été présentée par le Premier ministre le 16 octobre.**

Les grands axes de la stratégie nationale de sécurité du numérique

La numérisation de la société française s'accélère : la part du numérique dans les services, les produits, les métiers ne cesse de croître. Réussir la transition numérique est devenu un enjeu national. Vecteur d'innovation et de croissance, la numérisation présente aussi des risques pour l'état, les acteurs économiques et les citoyens. Cybercriminalité, espionnage, propagande, sabotage ou exploitation excessive de données personnelles menacent la confiance et la sécurité dans le numérique et appellent une réponse collective et coordonnée selon cinq objectifs stratégiques.

Intérêts fondamentaux, défense et sécurité des systèmes d'information de l'État et des infrastructures critiques, crise informatique majeure.

En développant une pensée stratégique autonome, soutenue par une expertise technique de premier plan, la France se donnera les moyens de défendre ses intérêts fondamentaux dans le cyberespace de demain. Parallèlement, elle continuera à renforcer la sécurité de ses réseaux critiques et sa résilience en cas d'attaque majeure en développant des coopérations tant à l'échelle nationale avec les acteurs privés qu'internationale.

Confiance numérique, vie privée, données personnelles, cybermalveillance.

Afin que le cyberespace reste un espace de confiance pour les entreprises de toutes tailles et les particuliers, des mesures de protection et de réaction seront adoptées. La protection passera par une vigilance accrue des pouvoirs publics sur l'utilisation des données personnelles et par le développement d'une offre de produits de sécurité numérique adaptée au grand public. La réaction s'articulera autour d'un dispositif d'assistance aux victimes de cybermalveillance qui apportera une réponse technique et judiciaire à de tels actes.

Sensibilisation, formations initiales, formations continues.

La prise de conscience individuelle des risques liés à la numérisation de la société reste insuffisante. Face à ce constat, la sensibilisation des écoliers et des étudiants sera renforcée. En outre, afin de répondre aux demandes croissantes des entreprises et des administrations en matière de cybersécurité, la formation d'experts dans ce domaine sera développée.

Environnement des entreprises du numérique, politique industrielle, export et internationalisation.
La croissance des marchés du numérique à l'échelle mondiale, et des exigences de sécurité qu'ils porteront, constituent une opportunité de différenciation pour les produits et services français ayant un niveau de sécurité numérique adapté aux usages. Par le soutien à l'investissement, à l'innovation, et à l'export, par le biais de la commande publique, l'État développera un environnement favorable aux entreprises françaises du numérique proposant une offre de produits et de services sécurisés.
Europe, souveraineté numérique, stabilité du cyberespace.
La régulation des rapports dans le cyberespace est devenue un sujet majeur des relations internationales.
La France promouvra, avec les États membres qui le souhaitent, une feuille de route pour l'autonomie stratégique numérique de l'Europe. Elle renforcera également son influence dans les instances internationales et soutiendra les pays volontaires les moins protégés dans la mise en place de capacités de cybersécurité afin de contribuer à la stabilité globale du cyberespace.
La sécurité du numérique conforte le projet de République numérique. L'État y joue un rôle majeur en élaborant cette stratégie et en lançant une dynamique dans laquelle les professionnels du numérique, les décideurs publics et privés et les citoyens sont invités à s'investir.
Source :
http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

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

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

Parce qu'il met en œuvre les moyens de la dissuasion nucléaire et qu'il conduit les interventions militaires en opérant 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 a une exigence particulière en matière de cyberdéfense.

Lancé en février 2014, le « *Pacte défense Cyber* » 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 concerne au-delà du seul ministère, les industriels et PME/PMI, les organismes de recherche et 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 et que 1 000 agents dédiés au cyber seront recrutés et affectés dans les états-majors, à la DGA, et dans les services de renseignement.

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

L'ANSSI s'associe aux actions engagées, notamment celles concernant l'axe 4.

(2) L'exercice « Defnet 2015 »

Exercice interarmées DEFNET 2015

L'exercice DEFNET organisé par le ministère de la défense au premier trimestre 2015 a permis de prolonger la coopération quotidienne du centre opérationnel de détection et de réponse aux attaques informatiques de l'ANSSI (COSSI) et de celui du ministère de la défense (CALID) ainsi que l'occasion de tester la mise en œuvre du déploiement de la réserve citoyenne à vocation opérationnelle cyber dont le pilotage est assuré par l'officier général cyberdéfense de l'état-major des armées.

Source : ANSSI

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

Les administrations de l'État sont des cibles potentielles pour les attaques informatiques.

Dès 2011, l'État 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'État**, est porté par les services du Premier ministre et notamment par 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'État est venu affirmer cette « unicité » du système d'information de l'État.

[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 de l'action publique.*

Sans tendre à l'uniformité, le but est de faire partager une même vision au sein des 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[1]. Le coût d'investissement correspond principalement à la mise en place du « cœur du réseau » à haut débit, avec l'installation d'équipement de routage à haut-débit, à hauteur d'environ 4 millions d'euros et d'infrastructure optique, à hauteur de 7,5 millions d'euros.

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. Le déploiement du RIE fluidifie les échanges interministériels, en particulier pour les sites de l'administration territoriale de l'État, qui sont enfin raccordés à un réseau commun. **Aujourd'hui il est déployé sur plus de 6 500 sites sur l'ensemble du territoire national.**

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

a) Des missions consolidées

Les missions de l'ANSSI sont définies par le décret du Premier ministre n°2009-834 du 7 juillet 2009 modifié[2] notamment en 2015 pour tenir compte des évolutions portées par les dispositions de la loi de programmation militaire de décembre 2013.

En 2011, l'ANSSI a publié une stratégie nationale de défense et de sécurité des systèmes d'information qui a mis en perspective les missions de l'agence regroupées en deux pôles :

- *un pôle de sensibilisation/prévention*, destiné à informer les différents publics des menaces présentes dans le cyberespace et des moyens de s'en protéger, et qui vise à garantir effectivement la sécurité des systèmes d'information des administrations et à contribuer à celle des opérateurs essentiels au bon fonctionnement de la Nation. Acteur « historique » en matière de prévention, l'agence renforce également sa politique de sensibilisation et de formation. Ses interventions dans le cadre de conférences et de colloques, bien au-delà du strict champ technique, participent à cette politique comme ses publications nombreuses ;

[1] *Hors coûts de raccordement des sites ministériels.*
[2] *http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212*

- *un pôle centré sur la réaction aux attaques et l'appui à la reprise de l'activité normale des systèmes d'information*. Le centre opérationnel de la sécurité des systèmes d'information (COSSI) est chargé de piloter la réponse de l'État et des entreprises nécessaires au bon fonctionnement de la Nation. L'anticipation des modes d'action ainsi que la détection et le traitement des attaques sont l'une des principales missions de l'agence.

La loi de programmation militaire de 2013 a confié de nouvelles missions à l'ANSSI en matière de protection des systèmes d'informations critiques des opérateurs d'importance vitale.

La stratégie numérique du Gouvernement, la stratégie nationale de sécurité du numérique et l'actualité opérationnelle entraînent un élargissement et une redéfinition des missions de l'agence actuellement en cours.

b) Une action amplifiée

(1) La protection de l'information de souveraineté

Depuis 2013, pour protéger les communications les plus importantes ou les plus secrètes des autorités, l'ANSSI continue de déployer des téléphones sécurisés TEOREM sur le réseau téléphonique ordinaire et sur le réseau RIMBAUD (réseau résilient destiné aux communications de crise).

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 et son extension. En complément des offres résilientes conçues avec un opérateur privé, le service ISIS a été également ouvert sur le *Réseau cœur gouvernemental* (RCG) opéré par le centre de transmissions gouvernemental (CTG) sur un ensemble de boucles optiques privatives. Au total, 230 sites sont raccordés à ce service. On comptabilise 2 300 abonnés, sur 900 postes, qui échangent très régulièrement (plus de 500 000 courriers électroniques).

Organisme militaire mis pour emploi fonctionnel auprès de l'ANSSI, le centre de transmissions gouvernemental (CTG) compte 180 personnels des trois armées. Il intervient dans la mise à disposition d'une partie des systèmes de télécommunications sécurisés nécessaires à la continuité de l'action de l'État, notamment celle de ses plus hautes autorités.

Une politique de sécurité des systèmes d'information de l'État (PSSIE), portée par la circulaire du 17 juillet 2014, fixe les règles de protection applicables aux systèmes d'information de l'État (voir supra p. 29).

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, notamment pour la communication ou l'échange d'informations sensibles.

(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'État. Les travaux d'amélioration du positionnement technique des systèmes de détection déjà en exploitation ont permis d'accroître encore le taux de couverture.

En parallèle, le centre de détection des attaques informatiques de l'ANSSI continue d'industrialiser les solutions développées et d'améliorer 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'État* (RIE).

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. Afin de mieux gérer une crise d'ampleur, l'organisation de crise de l'ANSSI a été affinée au premier semestre 2015 à la suite des attentats survenus à Paris en janvier et à la résolution de l'attaque informatique contre TV5Monde.

(3) La sécurisation des systèmes informatiques les plus sensibles

Devant la multiplication des attaques « critiques » qu'elle a dû traiter, l'ANSSI anticipe une augmentation des cas à court terme. Le déploiement plus large de solutions de détection contribuera très probablement à révéler de nombreux autres cas d'attaques qui aujourd'hui ne sont pas détectées.

Les dispositions de la loi de programmation militaire du 18 décembre 2013 relatives à la cyberprotection des opérateurs d'importance vitale ouvrent un vaste champ d'action pour l'ANSSI et dimensionnent ses travaux pour plusieurs années (voir supra p. 28). La publication des premiers décrets d'application de la loi et prochainement des arrêtés issus des concertations par secteur d'activité d'importance vitale et par famille de métiers avec les OIV en fournira le cadre. Si la concertation avec les OIV peut paraître longue, elle aura permis à l'ANSSI de mieux prendre connaissance leur spécificité et d'entreprendre une action de sensibilisation en profondeur qui sera probablement bénéfique dans la phase de mise en œuvre de leurs obligations. Elle permettra aussi à l'ANSSI de diffuser plus largement ces règles sous forme de recommandations à d'autres entreprises afin qu'elles puissent se protéger. Dans ce travail, elle pense pouvoir s'appuyer sur la directive européenne, en préparation, sur la sécurité des réseaux et des informations (*Network and Information Security – NIS*)

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

L'ANSSI a publié dans ces douze derniers mois 17 guides et notes techniques afin de sensibiliser les administrations, les acteurs économiques et le grand public. En outre, 33 articles scientifiques ont été publiés et 58 conférences scientifiques ou techniques prononcées dans des manifestations spécialisées.

L'ANSSI va également déployer un réseau de correspondants dans les régions afin de développer ses actions d'information et de conseil.

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. En 2014, neuf produits ont été qualifiés, certains pour la protection des informations classifiées au niveau *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. En 2014, l'agence a rencontré environ 300 industriels dans le cadre d'entretiens bilatéraux. Elle 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 des entreprises, à l'instruction de quatre projets retenus dans le cadre de l'appel à projets « sécurité numérique » et en cours de développement.

En 2014, l'ANSSI a piloté la finalisation de la feuille de route du 33ème plan de la *Nouvelle France Industrielle* (NFI). Le second semestre de 2014 et l'année 2015 ont été consacrés à la mise en œuvre de cette feuille de route.

Le centre de formation de l'ANSSI a reçu et formé 1.300 stagiaires durant l'année scolaire écoulée soit un nombre équivalent à l'année précédente.

Enfin, l'ANSSI a initié une politique de certification de prestataires compétents techniquement et de confiance, qui sont en mesure de soutenir les entreprises dans leurs efforts d'atténuation des risques et de résiliences aux cyberattaques. Elle a ainsi qualifié une vingtaine de prestataires d'audit de sécurité. À la mi-2016, elle publiera la liste des entreprises certifiées en matière de détection d'incidents et de réactions aux incidents. Cette qualification concerne à la fois les entreprises et leurs personnels.

Le développement d'un écosystème privé de cybersécurité est indispensable car l'ANSSI n'a ni la vocation, ni les moyens de tout faire tant les champs à couvrir ne cessent de s'étendre. Elle doit donc se concentrer sur ses missions et favoriser l'émergence de prestataires privés pour prendre le

relai dans la mise en œuvre de ses recommandations. Le cabinet d'étude Xerfi estime qu'en 2017 2 milliards d'euros seront dépensés sur le marché de la cybersécurité en France. Reste que la faiblesse du vivier des ingénieurs compétents freine le développement du secteur et que la convoitise des différents opérateurs pour s'en attacher les services n'est pas sans effet sur les difficultés rencontrées par l'ANSSI en matière de gestion de ses ressources humaines (voir infra p. 41).

(5) Audits

En 2014, les équipes de l'ANSSI ont réalisé plusieurs dizaines de prestations d'audit au profit de l'administration (64 %) ainsi que des opérateurs d'importance vitale privés (36 %).

Situations dans lesquelles des audits de l'ANSSI peuvent être réalisés

- au titre de l'inspection réglementaire du ministère de l'intérieur ;
- en application de l'article L. 33-10 du code des postes et des communications électroniques, qui prévoit l'obligation pour les opérateurs de communication électronique de se soumettre à des contrôles de sécurité à la demande du ministre chargé de l'économie ;
- en application de l'instruction générale interministérielle n° 6600 relative à la sécurité des activités d'importance vitale ;
- en lien avec l'assistance offerte par l'ANSSI à des services de l'État ou à des opérateurs OIV dans le cadre de la mise en œuvre de grands projets de système d'information ;
- à la demande de services de l'État, soit à leur profit direct, soit chez des opérateurs du secteur d'importance vitale dont ils assurent la tutelle ;
- au titre des opérations de cyberdéfense ;
- dans le cadre de la mise en œuvre de projets de systèmes d'informations internes à l'ANSSI.

(6) L'action internationale

Sur le plan multilatéral, l'ANSSI a participé aux travaux de l'ONU (*Groupe d'experts gouvernementaux* autour des questions de cybersécurité), de l'OCDE (groupe de travail « stratégies nationales de cybersécurité » et « vie privée et sécurité de l'information, WPISP), de l'OSCE (groupe sur les « *Confidence-Building Measures* » en matière de cybersécurité), de l'OTAN (notamment suivi et élaboration d'instructions pour les comités de l'OTAN s'intéressant à la cyberdéfense, élaboration des positions françaises en vue de deux réunions des ministres de la défense), de l'Union européenne (participation active à la négociation sur la stratégie européenne de cybersécurité[1], à la finalisation des *EU Standard Operating Procedures*,

[1] *Audition de M. Guillaume Poupard : « Dans le cadre des négociations sur la directive européenne pour la sécurité des réseaux, nous œuvrons pour que les autres pays européens aient l'obligation de se doter d'une structure homologue de l'ANSSI, dans l'optique de constituer un réseau d'agences. Nous incitons ainsi les pays qui ont actuellement une faiblesse dans ce domaine à développer cette*

négociation du mandat de l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), préparation des éléments relatifs à la cybersécurité des conclusions des Conseil numérique et défense, travaux de seconde évaluation des produits de sécurité protégeant des informations classifiées, etc.).

L'agence suit également de façon attentive la négociation des traités transatlantiques de façon à éviter que les données personnelles ne soient considérées comme des données marchandes. L'agrégation de masses de données personnelles peut également concerner la sécurité nationale.

Les relations avec les partenaires principaux se sont poursuivies en particulier avec le Maroc. L'ANSSI a engagé, en 2014, une coopération avec plusieurs pays d'Afrique sub-saharienne ainsi qu'un partenariat avec l'Inde en matière de cybersécurité.

(7) De nouveaux champs à explorer

Le développement de nouveaux usages et des objets connectés ouvre un nouveau champ d'action pour l'ANSSI. Il s'avère en effet que les concepteurs de ces nouveaux produits ne se préoccupent qu'insuffisamment des risques de sécurité. Il y a donc un besoin évident d'identifier ces risques, de sensibiliser les entreprises et d'accompagner la montée en puissance de cet écosystème.

C. LES MOYENS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2016

Le budget du SGDSN dans le projet de loi de finances pour 2016 s'élève à **237,72 millions d'euros** en autorisations d'engagements **(**211,3 en 2015) et **232,19 millions d'euros** en crédits de paiement (243,1 en 2015) **et un plafond de 895 ETPT.**

capacité et nous faisons du « capacity building », c'est-à-dire l'aide au développement. Il est en effet dans notre intérêt que ces maillons faibles de la cybersécurité améliorent leur protection : leur vulnérabilité est aussi la nôtre, les attaquants entrant souvent dans les réseaux par les pays les moins protégés. Enfin, le développement d'une capacité autonome européenne dans le domaine du numérique figure parmi les cinq axes de la stratégie nationale de sécurité publique. Ceci va au-delà de la cybersécurité ; il s'agit d'identifier les technologies-clefs qu'il est nécessaire de maîtriser en Europe afin de pas être dépendants des États-Unis ou de la Chine. » http://www.senat.fr/compte-rendu-commissions/20151012/etr.html#toc4

CRÉDITS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2016

(EN MILLIONS D'€)

	Exécution 2014 *		**LFI 2015**		**PLF 2016**	
	AE	CP	AE	CP	AE	CP
Titre 2	*47,66*	*47,66*	*64,29*	*64,29*	*66,76*	*66,76*
HT2	*127, 89*	*126,52*	*144,42*	*176,23*	*170,96*	*165,43*
TOTAL	192,12	194,17	**211,29**	**243,10**	**237,72**	**232,19**

**Hors transfert du Centre de transmission du Gouvernement (CTG)*

L'évolution du budget du SGDSN continue de s'inscrire principalement dans la priorité, portée par l'ANSSI, de **montée en puissance de la politique de sécurité des systèmes d'information et de protection des intérêts nationaux contre la cybercriminalité**, et confirmée par la loi de programmation militaire 2014-2019.

L'ANSSI représente désormais plus de la moitié des effectifs budgétaires (507 ETPT), et des efforts d'investissement ainsi que 70% des crédits de fonctionnement du SGDSN. Cette proportion augmentera avec sa montée en puissance.

Pour autant, elle ne constitue pas un BOP autonome. Au sein du SGDSN, le service d'administration générale assure par délégation du Secrétaire général l'ensemble des rôles et fonctions comptables et budgétaires pour l'ensemble des directions et services soutenus par le BOP SGDSN dont fait partie l'ANSSI. ; il en va de même pour le Centre des transmissions gouvernementales (CTG).

1. L'évolution des dépenses de personnel (Titre 2) suit la même évolution.

EFFECTIFS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2016

	LFI 2015		**PLF 2016**	
	ETP	ETPT	ETP	ETPT
ANSSI	483	455	523	507
CTG	184	184	184	184
SGDSN hors ANSSI et CTG	210	205	209	204
Total SGDSN	877	844	916	895

Le plafond d'emplois du SGDSN (hors ANSSI), relevant des orientations du Premier ministre pour les secteurs non prioritaires, **subira une diminution d'un emploi par an sur la période 2015-2017.** En outre, depuis 2015, sont rattachés les effectifs (184) du Centre de transmission gouvernemental (CTG), unité militaire mise pour emploi auprès du SGDSN.

La poursuite des créations d'emplois au profit de l'ANSSI sur la période triennale 2015-2017 est confirmée. Le schéma d'emploi de l'ANSSI pour la période est fixé à +145 ETP, dont +40 ETP en 2016. **Le plafond d'effectifs de l'ANSSI** fixé à 455 ETPT en loi de finances initiale pour 2015 **est porté à 507** en 2016 et 563 à échéance fin 2017. **Cette montée en puissance constitue un défi structurel de l'agence** qui doit également pourvoir au *turn over* relativement important de ces agents dont nombre sont, compte-tenu de leur spécialité, des contractuels. Elle doit à la fois recruter en nombre et maintenir le niveau qualitatif de ce recrutement. Comme l'indique le directeur général de l'ANSSI, M. Guillaume Poupard, entendu par votre commission : « *Nous recrutons beaucoup mais notre volonté est de ne pas abaisser le niveau de recrutement. Nous avons besoin d'experts et nous sommes confrontés à un problème d'insuffisance du vivier. La formation française est qualitativement bonne, mais quantitativement insuffisante. Nous avons des actions pour favoriser la mise en place de filières de formations, mais il faut du temps. Nous avons en attendant besoin de plus de souplesse de gestion et de pouvoir lisser dans le temps les recrutements qui n'ont pu être réalisés, une trentaine, au cours de l'exercice 2015, en nous autorisant la capacité de conserver les emplois créés, même s'ils ne sont pas encore pourvus* ».[1]

Si le recrutement à la sortie des grandes écoles et des universités demeure relativement aisé, malgré la faiblesse du vivier de formation, en raison de la bonne réputation de l'ANSSI dans le domaine de la cybersécurité. Le maintien de cadres et de techniciens expérimentés, pourvus d'une expérience incomparable est plus problématique compte tenu des rémunérations offertes par le secteur privé malgré l'existence de procédure permettant la transformation des CDD en CDI et la souplesse dont elle bénéficie pour fixer le niveau de rémunération. Le départ d'agents de l'ANSSI peut permettre également l'émergence d'un réseau lorsque les industriels qui embauchent ces personnels sont considérés comme de confiance.

Vos rapporteurs estiment que face à ces difficultés spécifiques, l'ANSSI doit être soutenue, en pérennisant les emplois autorisés mais non pourvus lors de la fixation des plafonds d'emplois en loi de finances afin de lui permettre de lisser les recrutements et en maintenant une certaine souplesse au niveau des rémunérations susceptibles d'être servies pour des contrats à durée indéterminée lorsque la qualité du recrutement ou de la pérennisation dans l'emploi le justifie.

[1] http://www.senat.fr/compte-rendu-commissions/20151012/etr.html#toc4

À plus long terme, une politique active de développement de filières de formation en écoles d'ingénieurs et en universités doit être conduite. La faiblesse du vivier est inquiétante d'autant que de nombreuses administrations de la défense, de l'intérieur, de l'économie et des finances, d'autres services du Premier ministre (comme le GIC) ou soutenus par lui comme la nouvelle CNCTR ou la CNIL recherchent des profils analogues ou voisins, sans parler des entreprises du secteur privé de plus en plus sensibilisées à la cybersécurité et souhaitent renforcer leurs direction des systèmes d'information ou d'entreprises de prestations de services spécialisées dans ce domaine.

Au schéma d'emploi net à +39 ETP en 2016 (soit + 40 pour l'ANSSI, -1 pour le SGDSN hors ANSSI) s'ajoute une réduction du plafond des opérateurs – 1 pour l'INHESJ) et – 2 pour l'IHEDN.

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

Les crédits hors titre 2 du SGDSN en PLF 2016 sont de 170,96 millions d'euros en AE et de 165,43 millions d'euros en CP.

Crédits hors titre 2 du SGDSN

HT2	LFI 2015		PLF 2016	
	AE	CP	AE	CP
Soutien et administration générale	10 430 311	11 076 312	8 964 002	9 235 886
CTIM	58 733 044	79 825 741	70 578 000	70 578 000
ANSSI	57 810 483	67 886 767	74 599 217	68 800 882
Opérateurs	17 446 500	17 446 500	16 817 500	16 817 500
TOTAL	**144 420 338**	**176 235 320**	**170 958 719**	**165 432 268**

Source : réponse au questionnaire parlementaire

L'ANSSI représente une part importante des crédits hors titre 2. Les dotations de l'ANSSI sont passées de 25,3 millions d'euros en loi de finances initiale pour 2009 à 68,8 millions en le PLF 2016. Elle progresse en crédits de paiement (1,5 %) comme en autorisations d'engagement (+29 %) alors que les crédits des autres postes diminuent.

Hors ANSSI, le SGDSN dispose de 96,6 millions d'euros en crédits de paiements pour 2016, soit une diminution sensible de 10,8 %. On observe une évolution inverse pour les autorisations d'engagement qui progressent de 10 % et s'élèvent à 96,4 millions d'euros. Au sein de cette enveloppe, les crédits destinés au soutien et à l'administration générale du SGDSN, c'est-à-dire ceux consacrés effectivement à son fonctionnement, s'élèvent à 9,2 millions d'euros et subissent une érosion sensible. Pour le reste, les écarts sont essentiellement la conséquence de l'évolution des crédits consacrés à la poursuite de projets interministériels concourant à la défense et à la sécurité nationale transférés en cours d'exercice vers le ministère de la défense.

a) Dépenses de fonctionnement.

(1) Dépenses de fonctionnement autres que celles de personnel.

Les crédits de fonctionnement destinés aux directions et services soutenus par le SGDSN qui s'élèvent à 53,4 millions d'euros d'AE et 53,3 millions d'euros de CP permettent de couvrir les dépenses et actions suivantes :

- le financement d'études dans le domaine de la sécurité des systèmes d'information (SSI), de projets en recherche et développement de systèmes de communication sécurisés et d'activités de prévention et de défense des systèmes d'information pilotés par l'ANSSI pour les besoins des autorités gouvernementales, des services de l'État et des opérateurs d'importance vitale pour un montant de 4,5 millions d'euros d'AE et de 2,7 millions d'euros de CP ;

- les dépenses de développement[1], de déploiement, de maintenance et de fonctionnement opérationnel des réseaux et systèmes de communication sécurisés mis à la disposition du gouvernement et des services de l'État, pour un montant prévu de 12,5 millions d'euros d'AE et en CP. Il s'agit des réseaux et systèmes sécurisés interministériels développés et soutenus par le SGDSN, et ceux développés et exploités par le Centre de transmission gouvernemental (CTG) ;

- l'acquisition[2] et la maintenance d'équipements informatiques et de réseaux locaux associés des systèmes d'information internes de l'ANSSI pour un montant prévu de 5,6 millions d'euros d'AE et de 4,6 millions d'euros de CP ;

- l'acquisition[3] et la maintenance des équipements de sécurité informatique (chiffreurs) des réseaux et systèmes de communication sécurisés pour un montant de 2 millions d'euros d'AE et en CP ;

- le financement d'activités interministérielles dans le domaine de la défense et de la sécurité nationale, **dont le SGDSN assure la coordination**, et notamment la réalisation d'études d'évaluation sur la résilience du territoire national et les menaces à l'encontre de la population, l'élaboration, la rénovation et la diffusion de plans gouvernementaux en matière de prévention et de gestion de crise contre le terrorisme et les actes malveillants, la réalisation d'exercices nationaux de simulation de gestion de crise majeure et le maintien en condition des moyens de veille et d'alerte au profit des autorités gouvernementales dans ces domaines, pour un montant prévu de 1,3 million d'euros d'AE et en CP ;

---

[1] *Pour les dépenses non immobilisées.*
[2] *Pour les dépenses d'équipement non immobilisées.*
[3] *Pour les dépenses d'équipement non immobilisées.*

- le financement de projets en recherche et développement de systèmes et équipements dans le domaine de la prévention des risques nucléaires, radiologiques, biologiques, chimiques et explosifs (NRBC-E), pour un montant prévu de 2,4 millions d'euros d'AE et en CP. L'effort est axé, d'une part, sur la poursuite du développement de la connaissance des procédés et de caractérisation d'explosifs artisanaux et, d'autre part, sur le développement des moyens de détection et d'intervention adaptés au profit du détachement central interministériel d'intervention technique ;

- les baux et dépenses immobilières (non immobilisées) des locaux occupés par les directions et services soutenus par le SGDSN, pour un montant prévu de 4,2 millions d'euros en AE et de 7,4 millions d'euros en CP. Les sites domaniaux sont exempts de loyer budgétaire. Le loyer et les charges locatives des locaux occupés par l'ANSSI sont évalués en 2016 à 2,6 millions d'euros CP (couverts par l'engagement réalisé lors de la prise à bail). Les dépenses d'entretien, fluides et services immobiliers (dont le nettoyage des locaux) de l'ensemble des locaux occupés en 2016 par les directions et services soutenus par le SGDSN sont estimés à 4 millions d'euros en AE et en CP ;

- les autres dépenses de fonctionnement courant des directions et services soutenus par le SGDSN, pour un montant de 6,9 millions d'euros en AE et 6,8 millions d'euros en CP. Ce poste de dépense comprend :

- d'une part, les dépenses consacrées à l'informatique non spécifique et à la bureautique, l'acquisition de serveurs et d'équipements actifs de réseaux, les dépenses d'entretien des réseaux locaux, l'acquisition et la maintenance de logiciels bureautiques ou spécifiques dans le domaine du soutien des services, ainsi que des besoins d'informatique courante (ordinateurs, périphériques et consommables).

- d'autre part les abonnements et frais de télécommunication ainsi que les frais de connexion sur différents réseaux, les frais de mission des agents, la contribution aux frais de restauration des agents sur les sites occupés par le SGDSN, qui représentent l'essentiel des crédits d'action sociale en faveur du personnel, et diverses autres dépenses courantes (mobiliers, fournitures, achats de documentation, etc.).

(2) Subventions pour charge de service public.

Deux instituts placés sous la tutelle du SGDSN relèvent de l'action 02 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).

Les subventions aux opérateurs sont prévues à hauteur de 16,8 millions d'euros dans le PLF pour 2016 à comparer avec 17,4 millions d'euros en loi de finances initiale pour 2015.

La diminution de 2 % de ces subventions par rapport à 2015 s'inscrit dans le cadre du budget triennal 2015-2017 sur l'évolution des crédits des opérateurs. L'effort d'économie demandé aux instituts pourra s'appuyer sur le renforcement des synergies et mutualisations entre les deux établissements de formation colocalisés à l'École militaire (voir infra p. 48).

b) Dépenses d'investissement.

Les crédits d'investissement du SGDSN, d'un montant de 99,6 millions d'euros en AE et de 94,1 millions d'euros en CP, sont consacrés essentiellement à des projets de défense et de sécurité nationale portant sur les domaines suivants :

- le développement et l'acquisition de systèmes et réseaux de communication sensibles et sécurisés au profit du gouvernement et des services de l'État ;

Un montant de 2 millions d'euros d'AE et de 3,5 millions d'euros en CP sera consacré au développement et à la modernisation des systèmes et réseaux de communication gouvernementaux sécurisés, principalement avec la poursuite du programme de modernisation du réseau Intranet sécurisé interministériel pour la synergie gouvernementale, du développement de services de visioconférence sécurisée, du développement des moyens des liaisons gouvernementales et voyages officiels, du programme de système interministériel de messagerie sécurisée, du projet d'hypervision des systèmes d'information et de communication sécurisés gouvernementaux et du programme interministériel de cryptophonie de nouvelle génération.

- le développement et l'acquisition de produits de sécurité informatique, principalement en vue de la protection des réseaux gouvernementaux, et le renforcement de la capacité de détection et de défense contre les risques du cyberespace ;

Un financement de 6,5 millions d'euros d'AE et de 10,6 millions d'euros de CP est prévu pour le développement et l'acquisition de produits de sécurité informatique. Ce poste comprend l'acquisition de chiffreurs pour les moyens de communication gouvernementaux et la poursuite du programme interministériel de modernisation des produits de sécurité des communications électroniques.

Un montant de 1 million d'euros d'AE et de 0,6 million d'euros de CP est prévu pour des projets immobilisés liés à la sécurité des systèmes d'information tant dans le domaine du développement de l'expertise technique, principalement pour les besoins des laboratoires de l'ANSSI, que dans celui de la prévention et de la défense des systèmes d'information contre les cyberattaques, avec le développement et l'acquisition de matériels et de logiciels spécifiques nécessaires aux missions du centre opérationnel de la sécurité des systèmes d'information (COSSI), et en particulier le centre national de crise cyberdéfense.

Un montant de 0,3 million d'euros en AE et de 0,4 million d'euros en CP est prévu pour le financement de moyens interministériels de défense et de sécurité nationale dont l'acquisition d'équipements d'intervention pour les besoins du détachement central interministériel d'intervention technique.

- la réalisation d'un centre d'hébergement de données (« data center ») avec le ministère de l'intérieur et une partie interministérielle;

Un montant de 19,2 millions d'euros en AE et 8,4 millions d'euros en CP sera consacré aux dépenses immobilières dont 16,1 millions d'euros et 8,5 millions d'euros de CP pour la réalisation d'un « data center » sera cofinancé avec le ministère de l'intérieur, maître d'ouvrage, et sera livré au plus tard en 2019. Le SGDSN participe au financement à hauteur de 75 %.

La réalisation d'un « data center » sécurisé

Le SGDSN conduit actuellement, conjointement avec le ministère de l'intérieur, les études préalables en vue de la création pour les besoins de l'ANSSI d'une salle de serveurs sécurisée - contiguë à des installations de même nature du ministère de l'intérieur - qui sera réalisée au sein d'un bâtiment existant en région parisienne. Cette opération nécessite une réhabilitation complète et une adaptation immobilière à ce type d'utilisation spécialisée.

La phase d'études et de définition du programme de chaque commanditaire devrait s'achever à l'automne. La notification du marché de maîtrise d'œuvre est prévue fin 2015 et celle du marché de travaux est planifiée fin 2016 pour une livraison de l'ouvrage début 2018. Le démarrage opérationnel des moyens techniques destinés aux besoins de l'ANSSI devrait intervenir à l'été 2018.

Le coût global de l'opération immobilière (livraison salle « sèche ») est estimé à 24,2 millions d'euros (TTC) et la quote-part de financement à la charge du SGDSN est évaluée à 18,2 millions d'euros.

- le développement de moyens interministériels dont ceux destinés à la prévention des risques nucléaires, radiologiques, biologiques, chimiques et explosifs (NRBC-E) ;

- enfin, 70,5 millions d'euros d'AE et CP seront consacrés à **la poursuite de projets interministériels concourant à la défense et à la sécurité nationale**. La dotation affectée aux programmes interministériels (CTIM) s'inscrit dans le cadre de la programmation pluriannuelle établie en 2013 et actualisée du taux d'inflation. Cette enveloppe devrait permettre de renforcer les programmes par des développements supplémentaires. Les crédits sont transférés en cours d'exercice vers le ministère de la défense.

c) Dépenses d'intervention

Il est prévu une dotation de 0,2 millions d'euros en AE et en CP sur le budget de l'ANSSI, cogérée par BpiFrance, à destination des petites et moyennes entreprises du secteur de la sécurité des systèmes d'information. Cette dotation est destinée à soutenir, tant en France qu'au niveau européen,

des projets d'innovation à composante technologique, présentant des perspectives concrètes de commercialisation, développés par des PME-PMI dans le domaine de la sécurité des systèmes d'information.

Une dotation d'un million d'euros en AE et en CP est par ailleurs destinée au cofinancement, dans le cadre du fonds unique interministériel (FUI), de projets de recherche, notamment dans le domaine de la protection contre le terrorisme ou la cybersécurité.

Ces projets intéressent directement les entreprises de la filière industrielle de sécurité regroupés au sein du comité de la filière industrielle de sécurité (CoFIS).

D. LES INSTITUTS NATIONAUX PLACÉS SOUS LA TUTELLE DU SGDSN

Les subventions pour charges de service public des deux opérateurs de l'État, placés sous la tutelle du SGDSN s'élèvent :

- pour l'Institut des hautes études de défense nationale (IHEDN), à 8,1 millions d'euros en AE et en CP ;

- pour l'Institut national des hautes études de la sécurité et de la justice (INHESJ) à 8,7 millions d'euros en AE et en CP.

Cette baisse est conforme aux orientations générales du Gouvernement de diminution de 2 % du montant de la subvention aux opérateurs de l'État L'effort d'économie demandé est une incitation supplémentaire à la recherche de synergies et de mutualisations entre ces deux établissements de formation co-localisés désormais sur le site de l'École militaire à Paris.

1. 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 pour sensibiliser, former et faire rayonner l'esprit de défense.

a) Une redéfinition des orientations stratégiques

L'IHEDN redéfinit ses orientations stratégiques pour s'adapter à un contexte de défense et de sécurité qui a fortement évolué. Ces orientations auront vocation ensuite à être formalisées dans un projet d'établissement et un contrat de performance actualisés. Elles seront soumises au Conseil d'administration le 18 novembre 2015. Elles s'articulent autour de quatre éléments :

- la volonté d'ouverture vers un public moins acquis, voire ignorant des questions de défense et de sécurité nationale[1], vers les jeunes générations et, plus largement, vers la société civile dans le cadre du lien citoyenneté-défense ;

- la structuration de la communauté de l'IHEDN, composée des auditeurs, des associations et des partenaires institutionnels ;

- l'information et la transmission de l'esprit de défense, de la connaissance de l'institution militaire, de ses enjeux, de la pensée stratégique française, par la mise en relation de l'ensemble des acteurs publics et privés engagés dans la mission de formation à la défense et à la sécurité globale ;

- la modernisation et la rationalisation de la gouvernance de l'institut, outil nécessaire à cette dynamique stratégique.

L'IHEDN entend poursuivre les relations avec ses partenaires ministériels mais également le Conseil supérieur de la formation et de la recherche stratégique (CSFRS) et l'Institut national des hautes études de la sécurité et de la justice (INHESJ). Il continue par ailleurs à apporter un soutien à la recherche universitaire par la délivrance de prix pour des thèses de doctorat et des mémoires de Master 2. Le fonds de dotation du cercle des partenaires soutient ainsi deux chaires universitaires.

Ces orientations impliquent un effort de modernisation pour l'Institut qui porte notamment sur l'adaptation et la rationalisation de son organisation et le renforcement de la mutualisation avec l'INHESJ, notamment sur le soutien, en favorisant des synergies pédagogiques, sans préjudice du caractère propre à chaque institut.

Selon les réponses au questionnaire parlementaire : « *le contrat de performance s'inscrira dans la démarche de modernisation des services de l'État et de ses opérateurs. Il fixera des objectifs principaux associés à des résultats à atteindre sur la base d'indicateurs de mesure ou de pilotage de la performance. De plus, en application du décret n°2012-1246 du 7 novembre 2012 relatif à la gestion budgétaire et comptable publique*[2]*, l'IHEDN doit mettre en place une comptabilité budgétaire distincte de la comptabilité générale dès le 1er janvier 2016. Cette évolution implique la mise en place d'un véritable projet de transformation qui rend nécessaire la mobilisation des responsables de l'établissement.* »

---

[1] *L'ouverture de l'établissement à un public plus large, ne connaissant pas ou peu les institutions, implique en particulier d'aller à la rencontre des jeunes issus de milieux moins sensibilisés aux questions de défense. Dans cette perspective, l'IHEDN à déployer sa présence en régions directement ou par des relais locaux.*

[2] *L'IHEDN a été retenu comme organisme pilote d'un nouveau mode de gestion budgétaire et comptable des établissements publics (GBCP). Ceci va modifier la présentation des documents budgétaires et comptables.* http://www.cegid.fr/secteurpublic/qu-est-ce-que-la-gbcp/r1-5982.aspx

b) Dans un cadre budgétaire resserré

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.

Le montant de la subvention annoncée pour 2016 est de 8,072 millions d'euros Comme pour les autres opérateurs de l'État, l'IHEDN supporte une diminution de 2 % par rapport à 2015 ; en outre deux emplois seront supprimés, le nombre d'ETPT autorisé revenant à 94. On notera que 5 emplois dont les trois emplois de direction sont rémunérés par d'autres ministères (défense, intérieur et affaires étrangères).

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

En 2013, l'IHEDN a pris en compte la poursuite de l'effort engagé en matière de fonctionnement (5,5 %) et la suppression de 3 emplois, conformément aux directives exposées dans la lettre de cadrage. Il a également subi en fin d'année un surgel (440 000 €).

En 2014, des efforts supplémentaires ont été demandés de 3,5 % sur la partie fonctionnement ainsi que deux emplois au titre de l'effort de productivité et 4 emplois supplémentaires dans le cadre de la modernisation de l'action publique. En fin d'année 2014, une modification budgétaire a eu pour objet de prendre en compte la diminution de la subvention pour charges de service public qui est passé de 8,554 millions d'euros en loi de finances initiale pour 2014 à 7,031 millions au compte financier, conformément au schéma de fin de gestion des services du Premier ministre après application de la mise en réserve de 193 102 euros en budget initial, application d'un surgel de 312 000 euros en cours d'année et d' un prélèvement du fonds de roulement de 1 million d'euros.

Les ressources propres n'ont pas compensé cette moindre contribution mais elles progressent de 3,9 % pour atteindre 1,92 million d'euros, soit 119.000 euros au-delà de la prévision inscrite au budget initial. Ceci est la conséquence de l'effort qui a été engagé en 2013 sur la recherche de recettes nouvelles et a été poursuivi depuis 2014. Les frais d'inscription sensiblement en hausse depuis 2013, ainsi que la sélection d'auditeurs pour lesquels la tarification est la plus élevée, ont permis d'enregistrer plus de recettes pour les sessions nationales « Politique de défense » et « Armement et économie de défense ». De plus, le tarif de la formation pour les entreprises de plus de 10 000 salariés est passé de 10 000 € à 15 000 €. Enfin, le conseil d'administration a décidé de rendre payantes les sessions régionales jusqu'alors intégralement gratuites. En revanche la collecte de la taxe d'apprentissage (83 120 euros) a été moins bénéfique qu'en 2013

(- 23,5 %) en raison de l'évolution de la législation. L'exercice a été soldé avec un déficit de 312 052 euros. **Cette instabilité en cours d'exercice du niveau de la contribution pour charges de service public qui représente 80 % des recettes ne permet pas une gestion cohérente de l'établissement.**

En 2015, la situation ne s'est guère améliorée avec une mise en réserve dès le budget initiale de 223 291 € sur une attribution de 8 002 209 euros en loi de finances initiale. Les évolutions réglementaires du droit individuel à la formation ont modifié sensiblement les prévisions de recettes au titre de la taxe d'apprentissage de 90 000 euros dans le budget initial à 50 697 euros dans le budget rectificatif. Le budget initial a été adopté avec un déficit prévisionnel de 117 202 euros.

Pour 2016, il est d'ores et déjà prévu une mise sous réserve de l'ordre de 187 749 euros et une recette de taxe d'apprentissage de 52 000 euros. L'équilibre reposera une nouvelle fois sur la capacité de l'IHEDN à réduire ses dépenses et à collecter des ressources propres.

Vos rapporteurs estiment qu'après un travail de réflexion engagé depuis plusieurs années sur la stratégie et le financement de l'IHEDN, il est temps que les orientations stratégiques puissent être arrêtées et qu'un contrat de performance puisse être conclu entre l'État et l'établissement.

2. L'Institut national des hautes études de la sécurité et de la justice (INHESJ)

a) 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. 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.

Le plan stratégique 2015-2017, adopté en juin 2015 par son conseil d'administration, porte l'ambition de l'institut d'être l'opérateur de référence dans ses missions fondatrices. Ainsi, l'institut doit être un partenaire reconnu pour l'organisation de formations ainsi que pour la réalisation d'études, de recherches, d'actions de valorisation et de diffusion de ses travaux dans les thématiques relevant de son champ de compétence.

Cinq grands objectifs stratégiques ont été retenus :

- prendre en compte de façon transversale la dimension « justice » au sein de l'Institut et affirmer son positionnement de référent sur les

réflexions portant sur l'analyse des phénomènes criminels, la sécurité économique et la réponse aux risques et crises ;

- conforter l'attractivité et la qualité des formations dispensées ;
- consolider l'activité « études et recherches », intégrée dans un réseau de partenaires reconnus, notamment dans un cadre européen et international ;
- développer la visibilité de l'Institut ;
- positionner l'Institut comme un agrégateur de compétences et de capacités.

L'année 2016 permettra la mise en œuvre de ces grands objectifs déclinés à travers des actions qui devront être priorisées pour tenir compte des moyens budgétaires et humains mis à disposition.

L'Institut déménagera en 2016 dans un bâtiment entièrement rénové au sein de l'École militaire. Ce nouveau bâtiment hébergera un nouveau plateau de formation à la gestion de crise équipé des technologies de pointe en la matière. Ceci permettra de renforcer sa capacité de formation et d'accueil des auditeurs, à travers des espaces de formation performants.

À la suite de l'adoption du plan stratégique, l'institut a élaboré un projet de contrat de performance qui a été transmis en septembre au SGDSN. Selon les réponses au questionnaire parlementaire ; « *il fera l'objet d'un examen prochain, notamment en lien avec le projet de contrat de performance de l'IHEDN qui devrait parvenir en début 2016* ». **Vos rapporteurs comprennent qu'il soit nécessaire, compte tenu du rapprochement entre les deux établissements, de veiller à la cohérence des deux contrats de performance**.

b) 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'établissement. Une autre partie, plus marginale, des recettes, est constituée des produits des publications et de la perception de la taxe d'apprentissage.

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. Le budget modificatif notifié en novembre 2014 a été ajusté par prélèvement de 1,65 millions d'euros au titre de la contribution du programme 129 à l'opération immobilière de rénovation du bâtiment de l'École militaire, futur siège de l'institut, et par une mise en réserve supplémentaire de 80 000 euros. Enfin, un prélèvement de 1 million d'euros sur le fond de roulement a été opéré en fin de gestion, **ce qui a ramené à 6,37 millions le montant de la subvention pour charge de service public au compte financier.**

Ces réductions sont en partie compensées par une légère augmentation de ses **ressources propres**, en particulier celles associées à ses capacités de formation et d'étude, qui se stabilisent **à hauteur de 1,5 million d'euros - une autre partie étant le fruit de sous-location des locaux occupés à Saint-Denis - et par la réalisation d'économies en cours de gestion à hauteur de 0,4 million d'euros. Pour autant, l'exercice s'est achevé avec un déficit de 599 000 euros.**

En 2015, le budget d'un montant de 9,22 millions d'euros a été notifié à hauteur de 7,39 millions d'euros en budget initial pour tenir compte d'une mise en réserve de 370 000 euros et d'un prélèvement provisionnel de 1,454 millions d'euros au titre de la contribution à l'opération immobilière susvisée. Les évolutions réglementaires établies par le décret n° 2015-151 du 10 février 2015 modifiant diverses dispositions relatives à la taxe d'apprentissage, ont pour effet d'exclure l'INHESJ du dispositif de perception de la taxe d'apprentissage. Il est présenté un budget rectificatif en 2015 qui acte la non-perception de cette taxe alors qu'un montant de 30 000 euros avait été inscrit au budget initial. Enfin le budget rectificatif ajuste le montant de ressources propres à hauteur de 3 384 817 €, qui constitue une prévision fiabilisée par rapport à celle du budget initial.

En 2016, la subvention inscrite au projet de loi de finances s'élève à 8,7 millions d'euros. Le nombre d'ETPT autorisé diminue d'une unité, passant à 73[1] auxquels s'ajoutent 5 emplois rémunérés par l'État par d'autres programmes (dont le directeur, un préfet, des personnels des ministères de la justice, de l'agriculture, de l'économie et des finances) ainsi que deux emplois rémunérés par les collectivités territoriales (officiers de sapeurs-pompiers) mis à disposition contre remboursement.

Le montant notifié au budget initial devrait être de l'ordre de 6,8 millions d'euros. Les projections budgétaires, en matière de ressources propres liées à la formation et à la recherche, s'établissent à environ 1,6 million d'euros annuels en 2016 et 2017. Ce chiffre constitue une forte progression par rapport aux exercices précédents. **Vos rapporteurs espèrent qu'il pourra être réalisé.**

L'année 2016 sera également marquée par la fin du bail d'occupation de l'immeuble que l'INHESJ occupe à Saint Denis. Si la fin du bail entraîne une réduction significative en dépenses, la disparition du produit locatif lié aux baux de sous-location conduira néanmoins à redéfinir le mécanisme de financement du bâtiment rénové à l'École militaire au profit

[1] *Sur le plan de la politique RH, l'institut applique les contraintes posées par le schéma d'emploi. Celles-ci se traduisent par une réduction du plafond d'emploi de 1 ETP annuel en 2016 puis d'un autre ETP en 2017. En parallèle, l'institut s'est engagé dès 2015 dans une politique de rénovation de sa stratégie RH en privilégiant une démarche « métiers » qui s'inscrit dans le plan stratégique. Cette démarche, qui se poursuivra pleinement en 2016, s'applique autant sur la partie liée à l'activité de formation et de recherche, que sur la partie liée à la gestion administrative et au soutien*

de l'INHESJ, ce produit locatif ayant été généralement affecté au financement de ce bâtiment.

Enfin, à l'instar de l'IHEDN, l'Institut connaîtra une rénovation de son cadre budgétaire à compter de 2016.

3. 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'un schéma directeur informatique commun ;

- la mise en place d'un groupement de commande depuis le 1er janvier 2014 pour certaines acquisitions et une agence comptable unique ;

- 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 ;

L'axe de mutualisation aujourd'hui retenu consiste à mener des actions communes de formation et de diffusion des connaissances (colloques, séminaires et publications) afin d'inscrire les deux instituts dans une dynamique de convergence et d'enrichissement complémentaire.

Vos rapporteurs mesurent la portée de ce rapprochement dont ils estimaient dans leur précédent avis qu'il était cohérent avec le continuum dégagé dès le Livre blanc de 2008 entre la défense et la sécurité nationale, tout en conservant la personnalité propre de chacun des deux établissements. Ce rapprochement doit être l'un des axes des contrats de performance qui seront présentés et approuvés au premier semestre 2016.

Ils souhaiteraient que les rapporteurs pour avis puissent avoir communication de ce document avant qu'il soit soumis pour adoption au conseil d'administration comme c'est le cas dans d'autres domaines (les contrats d'objectifs et de moyens des établissements publics opérateurs de la diplomatie culturelle, ou encore les sociétés de programmes de l'audiovisuel public par exemple) **afin de formuler un avis même si cette consultation n'est pas rendue obligatoire actuellement par la loi.**

Il serait souhaitable également que ces contrats qui engagent les établissements sur la conduite de leur stratégie et sur la modernisation de leur gestion, soient également engageants pour l'État en termes de stabilité des ressources publiques apportées à l'établissement.

II. LES AUTRES CRÉDITS DU PROGRAMME 129 CONCERNANT LES ASPECTS DE DÉFENSE ET DE SÉCURITÉ.

L'action 2 « Coordination de la sécurité et de la défense » contient la dotation en fonds spéciaux des services spécialisés de renseignement et les crédits du Groupe interministériel de contrôle.

En outre, au sein du programme 129, des crédits inscrits à l'action n° 01 « Coordination du travail gouvernemental » soutiennent l'Académie du renseignement, créée en 2010, comme service à compétence nationale rattaché au Premier ministre.

A. LES FONDS SPÉCIAUX

1. Une enveloppe de 47,3 millions d'euros

Les fonds spéciaux sont consacrés au financement de diverses actions liées à la sécurité extérieure et intérieure de l'État qui ne peuvent être financés sur des crédits budgétaires. Ils s'élèvent à **47,3 millions d'euros** en autorisations d'engagement et en crédits de paiement dans le projet de loi de finances pour 2016[1] à comparer avec les 49,9 millions d'euros inscrits en loi de finances initiale pour 2015. Ils concernent les services de renseignement et le Groupement interministériel de contrôle (GIC). Ces dotations sont souvent majorées en gestion par des décrets pour dépenses accidentelles et imprévisibles.

Dans le projet de loi de finances pour 2016, le montant des fonds spéciaux a été diminué de près de 2,6 millions d'euros au bénéfice des crédits de titre 2, afin de régulariser les modalités de prise en charge budgétaire de la rémunération de certains personnels du Groupement interministériel de contrôle jusqu'à présent rémunérés sur fonds spéciaux (voir infra p. 57). Cette clarification est bienvenue.

2. Le contrôle de l'utilisation des fonds spéciaux

Le contrôle de l'utilisation des fonds spéciaux a été confié par le législateur (loi de finances pour 2002) à la Commission de vérification des

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

fonds spéciaux dont la composition a été modifiée par la loi de programmation militaire du 18 décembre 2013[1].

Dans le cadre plus général d'un approfondissement du contrôle parlementaire sur les services de renseignement, la CVFS est désormais une **formation spécialisée au sein de la Délégation parlementaire au renseignement.** 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 d'une unification des différentes facettes du contrôle parlementaire des services de renseignement.

B. LE GROUPEMENT INTERMINISTÉRIEL DE CONTRÔLE (GIC)

Le groupement interministériel de contrôle (GIC) est un service du Premier ministre chargé des interceptions de sécurité et du recueil des données de connexion.

Article R.242-2 du code de la sécurité intérieure

Le groupement interministériel de contrôle a pour missions :
1° de soumettre au Premier ministre les propositions d'interception présentées dans les conditions fixées par l'article L.242-1 du code de la sécurité intérieure;
2° d'assurer la centralisation de l'exécution des interceptions de sécurité autorisées ;
3° de veiller à l'établissement du relevé d'opération prévu par l'article L.242-4, ainsi qu'à la destruction des enregistrements effectués, dans les conditions fixées par l'article L.242-6.

La loi n° 2015-912 du 24 juillet 2015 relative au renseignement prévoit un éventail de techniques de renseignement, dont le processus d'autorisation et de mise en œuvre devra faire l'objet d'une traçabilité et d'une centralisation par le GIC. Le GIC restera l'interface indispensable entre les services autorisés et les opérateurs. Il devra mettre en œuvre les processus de demande et gérer les autorisations, garantir l'homogénéité des procédures de suivi, veiller à la conformité des interventions et utilisations des dispositifs aux autorisations accordées, et gérer le stockage des données et leur accès. Il devra offrir toute garantie de sécurité pour le transport, le traitement et la conservation des informations.

---

[1] *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.*

Ces missions nouvelles imposent un changement de dimension du GIC et plus généralement une refonte lui permettant de prendre en compte le contexte technologique complexe et de répondre aux nouvelles attentes du Premier ministre, des services de renseignement et de la Commission nationale de contrôle des techniques de renseignement (CNCTR).

En vue de répondre à ses nouvelles missions, le GIC devra augmenter le dispositif de stockage des données des interceptions de sécurité dont la durée de conservation autorisée passe de 10 à 30 jours, développer des dispositifs d'archivage et de traitement des données recueillies par les techniques de renseignement dont il assure la centralisation, et organiser par des guichets au sein de chacune des directions, des cabinets ministériels concernés dont celui du Premier ministre) et de la CNCTR, le système de demande d'autorisation et de contrôle des nouvelles techniques de renseignement.

Dans le cadre du projet de loi de finances pour 2016, le directeur des services administratifs et financiers du Premier ministre a demandé la création d'une sous-action 3 « GIC » sur l'action 2 du programme 129 pour suivre spécifiquement les crédits alloués au GIC, en dehors de l'exécution des fonds spéciaux.

1. Une évolution qui aura des conséquences en termes d'effectifs

Une partie du personnel du GIC est mise à disposition par le ministère de la défense. Au 31 décembre 2014, 75 postes budgétaires étaient armés par des militaires (officiers et sous-officiers des trois armées) et des civils du ministère de la défense (fonctionnaires et agents sous contrat). Au 30 juin 2015, l'effectif réalisé est de 73 agents. Le coût de cette mise à disposition s'est élevé à 4,6 millions d'euros en 2014 (CAS pensions inclus). Les crédits sont inscrits au programme 212 de la mission « Défense ».

En 2003, le GIC a été autorisé à recruter 60 agents sur contrats et vacataires, rémunérés sur crédits de fonds spéciaux. Au 31 décembre 2014, les effectifs employés étaient de 50 agents.

Le projet de loi de finances pour 2016 explique la hausse de 139 ETPT du plafond d'emplois pour partie par « un effet en ETPT **des mesures de périmètre pour 2016 (+ 60 ETPT) correspondant à la prise en charge, sur les crédits de titre 2 des personnels du GIC jusqu'à présent hors plafond d'emplois »**[1]. En outre, **pour tenir compte des besoins exprimés de renforcement des moyens suite à la promulgation de la loi du 24 juillet 2015, le plafond d'emplois du GIC est établi à 80 ETPT**[2]**.**

[1] *PAP du programme 129 p. 50.*
[2] *PAP du programme 129 tableau p. 52.*

En conséquence, le titre 2 est doté de crédits à hauteur de 3,9 millions d'euros[1] en AE et en CP. Les personnels contractuels du GIC seront donc à compter de 2016 rémunérés sur les crédits de la sous-action GIC créée à cet effet. Ce montant correspond pour 2,65 millions à des rémunérations d'activité pour 1,19 à des cotisations et contributions sociales (y compris les cotisations au CAS Pensions) et pour 0,06 à des prestations sociales et allocations diverses.

2. Une évolution positive des crédits de fonctionnement

Enfin, le GIC qui recevait depuis 2008 **des crédits destinés à couvrir ses dépenses de fonctionnement courant** ainsi que la rémunération des prestations fournies par les opérateurs de téléphonie mobile, à hauteur de 300 000 euros, verra ce montant **porté à 500 000 euros en 2016**.

Une partie du fonctionnement et les investissements nécessaires à la montée en puissance du groupement continueront à être financés par une attribution de fonds spéciaux.

C. L'ACADÉMIE DU RENSEIGNEMENT

La création de l'Académie du renseignement, en 2010[2], est, avec la mise en place d'un Coordonnateur national du renseignement, l'une des mesures décidées dans le cadre du renforcement du renseignement à la suite du Livre blanc sur la défense et la sécurité nationale de 2008, et de la constitution d'une véritable « **communauté du renseignement[3] »**.

Par sa mission de formation, l'Académie du renseignement contribue au renforcement des liens au sein de la communauté du renseignement. Elle organise au profit des services **une formation initiale** pour tous les cadres nouvellement affectés**, des séminaires spécialisés**, et **un cycle supérieur du renseignement**, destiné à des cadres supérieurs des services de renseignement. **Le nombre de personnes formées par l'Académie depuis 2010 est de l'ordre de plusieurs centaines[4].**

Outre ces actions de formation des cadres**, elle a développé des actions destinées à sensibiliser au renseignement d'autres publics : parlementaires et fonctionnaires des autres administrations.** Cette mission est complétée par des **manifestations publiques** (colloque, rencontres, etc.) et de **communication**. Plus généralement, l'Académie vise à développer sa

---

[1] *Le tableau p. 48 fait figurer ces crédits en autorisations d'engagement pour la sous-action « GIC » alors qu'ils demeurent en titre 2 de la sous-action fonds spéciaux en crédits de paiement en raison d'une erreur de saisie lors de l'élaboration du document.*

[2] *Décret n°2010-800 du 13 juillet 2010*

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

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

visibilité auprès du monde universitaire et des publics extérieurs à la communauté du renseignement, intéressés par cette thématique.

Service à compétence nationale rattaché au Premier ministre, l'Académie du renseignement est, du point de vue de son effectif et de son budget, une petite structure très légère. Elle emploie quinze personnes dont la directrice, son adjoint, et 4 conseillers pédagogiques. Ses crédits sont gérés par les services du Premier ministre (action n°01 « coordination du travail gouvernemental »). **Son budget de fonctionnement s'élevait en 2015 à 375 000 euros.** Les crédits de personnel représentaient quant à eux à **967 800 euros en 2014**.

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.

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 17 novembre 2015.

Après l'exposé des rapporteurs, **M. Jacques Gautier** a souligné l'importance du travail de coordination du SGDSN et rappelé la production d'une étude récente sur l'usage malveillant des drones de loisir.

La commission a ensuite donné un avis favorable, pour ce qui concerne le programme 129, à l'adoption des crédits de la mission « Direction de l'action du Gouvernement ».

ANNEXE I - AUDITION EN COMMISSION

Mercredi 14 octobre 2015

M. Louis Gautier, secrétaire général de la défense et de la sécurité nationale et M. Guillaume Poupard, Directeur général de l'agence nationale de la sécurité des systèmes d'information (ANSSI).

Compte-rendu consultable sur le site Internet du sénat à l'adresse suivante :
http://www.senat.fr/compte-rendu-commissions/20151012/etr.html#toc4