N° 142

SÉNAT

SESSION ORDINAIRE DE 2016-2017

Enregistré à la Présidence du Sénat le 24 novembre 2016

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* **2017**, *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 Émorine, 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, Yves Pozzo di Borgo, Henri de Raincourt, Alex Türk, Raymond Vall, Bernard Vera.

Voir les numéros :

Assemblée nationale (**14**ème législ.) : **4061, 4125** à **4132** et T.A. **833**

Sénat : **139** et **140** à **146** (2016-2017)

SOMMAIRE

Pages

LES PRINCIPALES OBSERVATIONS DE VOS RAPPORTEURS POUR AVIS

1. La demande de crédits inscrite dans le projet de loi de finances pour 2017 dans le programme 129 « Coordination du travail gouvernemental » est de 707,29 millions d'euros, soit 48 % 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 **350 millions d'euros** (327,31 en 2016) en autorisations d'engagement et de **345,40 millions d'euros** de crédits de paiement (315,291 en 2016).

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 du Groupement interministériel de contrôle (GIC).

Par rapport à la prévision inscrite en loi de finances initiale pour 2016, la dotation de cette action enregistre une **croissance de 9,5** % en CP (**- 30,1 millions d'euros**) comme en autorisations d'engagement (+ 7%, 22,68 millions d'euros) en raison de la poursuite de la montée en puissance de l'ANSSI et de l'adossement du GIC au budget opérationnel de programme.

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 des efforts d'investissement et des crédits de fonctionnement du SGDSN.

2.1. Le plafond d'emplois du SGDSN (hors ANSSI et CTG) se voit relevé de 6 ETPT supplémentaires.

La poursuite des créations d'emplois au profit de l'ANSSI est confirmée. Le plafond d'effectifs de l'ANSSI, fixé à 507 ETPT en loi de finances initiale pour 2016, est porté à 545 en 2017. 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 utile pour diffuser une « culture de la cybersécurité ». 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 continuer à être soutenue par la pérennisation des emplois autorisés mais non pourvus lors de la fixation des plafonds d'emplois en loi de finances, pour lui permettre de lisser les recrutements et qu'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, doit être maintenue.

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. **La politique de labellisation des filières de formation par l'Agence est une étape intéressante, mais une implication plus forte du ministère de la recherche et de l'enseignement supérieur et des partenaires économiques, est indispensable.**

2.2. L'ANSSI représente une part importante des crédits hors titre 2. **La réalisation d'un centre d'hébergement de données sécurisé représente le principal investissement.** Il est prévu en 2016 un transfert de 18,2 millions en AE et 5,3 millions en CP au profit du programme « Conduite et pilotage des politiques de l'intérieur » pour la réalisation de ce projet commun dont le ministère de l'intérieur est le maître d'ouvrage. **6,5 millions d'euros de CP sont inscrits à ce titre en 2017.**

3. Les subventions destinées à l'IHEDN et à l'INHESJ sont prévues à hauteur de 13,8 millions d'euros dans le projet de loi de finances pour 2017 à comparer avec 16,8 millions d'euros en loi de finances initiale pour 2016. Ces opérateurs sont en pleine restructuration, après l'élaboration d'orientations stratégiques, ils sont entrés en phase de négociation de contrats de performance avec l'État. L'INHESJ a conclu en mai 2016. Celui de l'IHEDN reste en cours de négociation. 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. Ils regrettent le retard pris dans la rédaction du contrat d'objectifs et de performances 2015-2017 de l'IHEDN qui risque de n'être qu'un exercice formel. **Ils estiment nécessaire de faire coïncider davantage les démarches stratégiques et contractuelles des deux Instituts s'ils doivent poursuivre la mutualisation de leurs moyens et la mise en cohérence de leurs missions. Puisque les contrats en vigueur ou en négociation s'achèveront en 2017, l'opportunité est offerte aux deux instituts de travailler de conserve et sous l'autorité du SGDSN, à la mise au point de contrats couvrant la période 2018-2020.**

4. Les fonds spéciaux s'élèvent à 67,8 millions d'euros. Cet ajustement accompagne la montée en puissance des services de renseignement dans la lutte anti-terroriste. Il correspond à une demande de la Commission parlementaire de vérification des fonds spéciaux dans son dernier rapport.

5. Pour l'application de la loi relative au renseignement de juillet 2015, l**e Groupement interministériel de contrôle (GIC),** jusqu'alors chargé d'exécuter les interceptions de sécurité et de recueillir les données de connexion, devient le pivot interministériel de gestion de l'ensemble des techniques et assure, pour leur mise en œuvre, un rôle de conseiller auprès du Premier ministre, et de correspondant privilégié de la CNCTR.

La place du renseignement dans la lutte contre le terrorisme entraîne dans le même temps une intensification de son activité.

Pour ce faire, il doit adapter ses structures et son organisation et réaliser un certain nombre d'investissements.

La révision du statut d'ensemble de son personnel a été initiée en cours d'année 2016 avec le rattachement effectif de son personnel au service du Premier ministre et par le transfert en 2017 des personnels militaires et civils qui, jusqu'alors, étaient mis à disposition par le ministère de la défense. Au total, le GIC disposera en 2017 de 189 ETP. A l'horizon 2020, il devrait employer 220 personnes.

Un effort budgétaire est réalisé pour accompagner sa montée en puissance. Les crédits hors titre 2 sont élevés à 16,6 millions d'euros, dont une moitié pour des investissements (acquisition de matériel informatique et réalisation d'infrastructures).

Vos rapporteurs mesurent l'ampleur et l'enjeu du processus de transformation en cours et se réjouissent des nouvelles modalités de gestion du personnel du Groupement et de l'évolution de son mode de financement. Ils souhaitent que le Premier ministre se montre particulièrement attentif pour assurer sa montée en puissance car elle constitue le point sensible de la mise en œuvre efficace de la loi relative au renseignement. Les modalités techniques de son adossement au SGDSN devront être rapidement précisées pour entamer la gestion de l'exercice 2017 sur des bases stables.

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 2017***.**

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 d'apprécier la gestion des services qui lui sont rattachés comme le centre des transmissions gouvernementales (CTG) ou l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dans le prolongement des travaux passés de votre commission sur la cyberdéfense[1] ; il permet notamment de suivre attentivement l'évolution des moyens et des effectifs attribués à cette agence.

Il complète, enfin, l'information de la commission sur le suivi des moyens interministériels affectés à la politique publique du renseignement, notamment au travers des moyens du Groupement interministériel de contrôle (GIC), qui s'est vu confié par la loi n° 2015-192 du 24 juillet 2015 relative au renseignement un rôle central dans l'instruction des demandes de mise en œuvre des techniques de renseignement, de la réalisation de certaines d'entre elles[2] et du contrôle de l'ensemble des procédures, des fonds spéciaux destinés aux services de renseignement, et de l'Académie du renseignement en charge d'actions de formation.

Enfin, il permet de prendre connaissance de la gestion des établissements publics dont il assure une grande partie du financement par le versement d'une contribution pour charge de service public, l'IHEDN et l'INHESJ.

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 2017 de **350 millions d'euros** (327,31 ouverts en loi de finances initiale pour

---

[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

[2] *Dans le cadre de la loi n° 91-646 du 10 juillet 1991, le GIC réalisait les interceptions de sécurité et dans celui de la loi n° 2006-64 du 23 janvier 2006, il accueillait, dans ses locaux, l'autorité en charge de la réalisation du recueil des données de connexion.*

2016) en autorisations d'engagement et **345,40 millions d'euros** de crédits de paiement en 2016 (315,29 en 2016), et qui représentent près de la moitié des crédits inscrits au programme 129.

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	2017 2016 2015	84 467 059 70 907 605 *61 995 478*	265 533 340 256 407 513 *165 383 576*	**350 000 399** **327 315 118** ***227 379 054***
Crédits de paiement	2017 2016 2015	84 467 059 70 907 605 *61 995 478*	260 936 845 244 381 062 *173 957 584*	**345 403 904** **315 288 667** ***235 953 062***

En euros.
Sources : 2015 autorisations et crédits consommés (rapport annuel de performances/loi de règlement), 2016 et 2017 : Projet annuel de performance / projet de loi de finances : loi de finances initiale 2016 et PLF 2017.

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

	LFI 2016		**PLF 2017**	
	AE	*CP*	*AE*	*CP*
SGDSN	***256 358 355***	***244 331 904***	***254 629 749***	***250 033 254***
Titre2	70 739 695	70 739 695	73 560 211	73 560 211
Hors titre 2	185 618 660	173 592 209	181 069 538	176 473 043
Fonds spéciaux	***56 794 717***	***56 794 717***	***67 856 000***	***67 856 000***
GIC	***18 144 136***	***18 144 136***	***27 514 650***	***27 514 650***
Titre2	4 150 000	4 150 000	10 906 848	10 906 848
Hors titre 2	13 994 136	13 994 136	16 607 902	16 607 902
Total action 2	**327 315 118**	**315 288 667**	**350 000 399**	**345 403 904**

Sources : LFI 2016 et 2017

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 ».

	LFI 2016		**PLF 2017**	
	AE	*CP*	*AE*	*CP*
Académie du renseignement (P129-01)	***355 000***	***355 000***	***N.C***	***N.C***
Titre 2	0	0	0	0
Hors titre 2	355 000	355 000	N.C	N.C

N. C : non connu à la date de la réponse

TITRE PREMIER : LE SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN) ET LES ENTITÉS RELEVANT DU PROGRAMME 129

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

Le SGDSN est l'outil du Gouvernement pour le traitement des sujets sensibles en matière de défense et de sécurité nationale. Son action recouvre les missions suivantes :

- coordination interministérielle ;

- planification de gestion de crise ;

- transmissions gouvernementales ;

- sécurité des systèmes d'information ;

- coordination technologique ;

- coordination des enseignements de défense et de sécurité;

- coordination du renseignement.

A l'heure où les attentats terroristes se sont multipliés sur le territoire national, le SGDSN a été fortement sollicité pour élaborer des réponses en terme de protection, en appui à la mission du Premier ministre, responsable de la défense nationale dont il dépend organiquement, et à celle du Président de la République, chefs des armées, qui préside le conseil de défense et de sécurité nationale dont le SGDSN assure le secrétariat. Il a donc en 2015, et plus encore en 2016, été particulièrement actif tout en assurant l'exécution de ses autres missions. **Ces deux années ont entraîné une intensification de son activité.**

A. LE SGDSN ASSURE LE SECRÉTARIAT DES CONSEILS DE DÉFENSE, MÈNE DES TRAVAUX D'ANTICIPATION STRATÉGIQUE ET ASSURE LE SUIVI DES CRISES INTERNATIONALES

1. Le secrétariat des Conseils de défense et de sécurité nationale

Présidé par le chef de l'État, en présence du Premier ministre, le conseil de défense et de sécurité nationale (CDSN) a compétence sur toutes les questions de défense et de sécurité : programmation militaire ou de sécurité intérieure, politique de dissuasion, sécurité économique et énergétique, lutte contre le terrorisme ou planification des réponses aux crises.

Outre sa configuration plénière, il comporte deux formations spécialisées, qui siègent dans une composition adaptée : le conseil national du renseignement et le conseil des armements nucléaires. Le premier définit les orientations et les priorités stratégiques, et planifie les moyens humains et techniques des services spécialisés de renseignement. Le second traite des différents aspects de la dissuasion nucléaire : doctrine, format des forces, programmes de simulation et d'armement, types d'armes... Le CDSN peut également se réunir en formation restreinte, en particulier pour évoquer les opérations extérieures.

Le code de la défense prévoit que le Secrétaire général assure le secrétariat de ces conseils. À ce titre, il prépare le dossier de ces réunions, dans une approche interministérielle, propose le projet de compte rendu qu'approuve le Président de la République, élabore les relevés de décisions, notifie les décisions prises et suit leur mise en œuvre. S'agissant des conseils nationaux du renseignement, le SGDSN intervient en appui du coordonnateur national du renseignement**. En 2015, le conseil de défense et de sécurité nationale s'est réuni à dix reprises. En 2016, le rythme des réunions a encore crû, notamment en raison des décisions à prendre à la suite des attentats terroristes sur le territoire national. Il est très supérieur à deux réunions par mois. La question du rythme de réunion du conseil est donc tout à fait importante pour le SGDSN.**

2. Le suivi des conflits et des crises internationales

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.

En 2015/2016, quatre sujets ont fait l'objet de travaux d'anticipation : le Levant, l'Afrique équatoriale, les flux migratoires touchant l'Europe et les trajectoires terroristes en Asie méridionale. En 2016/2017, les études porteront sur l'après *Daesh* (stabilisation et reconstruction en Irak et en Syrie), les Balkans occidentaux et le Sud-Est de l'Afrique.

3. Les questions de prospective et d'ordre stratégique

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. Ce comité se réunit une fois par an.

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**, comme par exemple à l'occasion du sommet de l'OTAN à Varsovie (8 et 9 juillet 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, en priorité, 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. La première phase du programme européen à laquelle la France participe activement devrait se terminer début 2017. La deuxième phase débutera dans le courant de l'année prochaine.

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. Cette stratégie a été remise à jour au printemps 2016.

Elle constitue l'amorce, par la France, d'une approche globale des crises dans les régions d'intérêt, là où elle est, ou est susceptible d'être, engagée militairement. Dans son rapport sur les interventions extérieures de la France[1], le groupe de travail de votre commission a souhaité un renforcement du rôle du SGDSN dans le pilotage de ces stratégies régionales, leur développement car elles sont limitées aujourd'hui au Sahel, alors que la France est engagée sur d'autres théâtres (Levant, RCA) et devrait développer préventivement une approche stratégique globale pour des régions exposées ainsi que la nomination de représentants spéciaux de théâtres chargés de piloter l'accompagnement des opérations civiles d'expertise, de coopération et d'aide au développement pendant la phase d'intervention militaire et de post-crise. **Vos rapporteurs demandent au Premier ministre d'expertiser ces propositions et de les mettre en œuvre.**

4. 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

[1] *Rapport d'information de la commission des affaires étrangères, de la défense et des forces armées du Sénat n° 794 (2015-2016) par MM. Gautier, Reiner, Bockel, Lorgeoux, Perrin et Roger, p. 215 à 218 - http://www.senat.fr/notice-rapport/2015/r15-794-notice.html*

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**, il 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 types P3 et P4.

Face à **la menace du risque chimique ou bactériologique**, le Premier ministre a mis en place, en 2015, **le Conseil national consultatif pour la biosécurité (CNCB)** dont la mission est d'éviter le détournement des recherches sensibles à des fins terroristes. Le pilotage de cette nouvelle instance a été confié au SGDSN. Il sera chargé, notamment, de proposer des mesures pour assurer la prévention et la détection d'éventuelles menaces, leur traitement et l'information du public. Il mènera des travaux de veille et de prospective sur les recherches à caractère dual et formulera des recommandations, afin que les progrès réalisés dans les sciences du vivant ne génèrent pas de menaces nouvelles.

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. Quatorze affaires d'interception de biens proliférant ont ainsi été menées dans ce cadre depuis l'été 2015. Depuis l'été 2016, le SGDSN assure également la coordination d'interceptions des armements conventionnels, dans un cadre strictement national.

5. 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, plus de 500 ZRR ont été créées.

6. 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 et assure pour la France la fonction d'Autorité responsable. Il est prévu que cette autorité se dote d'un cadre légal adapté à l'exercice de ses responsabilités pour la fin de l'année.

En 2015, ces travaux ont consisté notamment à finaliser avec la commission et nos partenaires européens 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 »).

Dans le cadre de la coordination interministérielle *GALILEO*, le SGDSN, sans préjudice des prérogatives du SGAE, est responsable de ces négociations internationales sur le PRS et anime un groupe de travail interministériel afin de définir les positions nationales relatives à ces négociations.

7. Le 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. Les discussions menées avec la commission en 2015, notamment sur la base de l'argumentaire fourni par la France, ont montré que la proposition de directive de la commission était inadaptée et ne répondait pas à une logique d'optimisation du marché commercial de l'imagerie satellitaire. La commission en a pris acte et n'a donc pas proposé de suite à cette initiative.

8. Le soutien à l'industrie nucléaire civile

Le SGDSN intervient à la demande des autorités politiques, sur des sujets ponctuels concernant la filière nucléaire civile dont l'instruction nécessite un travail interministériel approfondi. La filière nucléaire civile française met en jeu des problématiques de sécurité et de défense, tant sur le plan national qu'international, mais porte également des enjeux forts sur le plan économique et de la protection des technologies et savoir-faire nationaux. Le SGDSN s'est vu confier trois mandats de cette nature depuis un an.

Par ailleurs, il se voit confier des mandats sur une durée plus longue, correspondant à la durée de projets industriels de très grande envergure.

9. 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

Sur la période de juin 2015 à juin 2016, la CIEEMG a examiné 6 381 dossiers correspondant à 4 549 dépôts de nouvelles « demandes de licences » et 1 832 demandes de « modification de licences » déjà accordées (soit 40 %). Environ 95 % des demandes ont fait l'objet d'un traitement en procédure « continue »[1] avec avis favorable. Il faut noter que 50 % de ces demandes de licence ont été accordées avec des conditions particulières destinées à encadrer l'opération. La CIEEMG s'est réunie en session plénière à onze reprises pour l'examen de 278 dossiers pour lesquels elle a prononcé 160 avis favorables et 118 avis défavorables

Le SGDSN a lancé en 2016 les travaux de révision des « directives de haut niveau », qui servent de cadre méthodologique aux décisions proposées à l'exécutif par la CIEEMG dont la dernière édition remonte à mars 2015. Des travaux en cours ont pour objectif de mieux cibler les contrôles vers les pays sensibles et d'alléger le contrôle sur les matériels transférés vers des pays de l'Union européenne. Parallèlement, le ministère de la défense pourra désormais infliger des amendes aux entreprises défaillantes en matière d'organisation interne ou de contrôle des exportations.

Il a également piloté différents travaux interministériels d'adaptation de la réglementation en matière de contrôle d'armements[2] ou de mise en conformité de celle-ci par rapport à nos engagements internationaux[3]. Il apporte son expertise à la commission interministérielle des biens à double usage (CIBDU) pour l'instruction des dossiers sensibles.

En matière de réglementation européenne, le SGDSN a coordonné les travaux concernant la directive européenne 2009/43 du 6 mai 2009 sur les transferts intracommunautaires des produits liés à la défense (dite directive TIC), notamment ceux visant à renforcer la mise en œuvre des licences générales de transfert à destination des forces armées et des entreprises

---

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

[2] *Projet d'ordonnance d'élargissement des compétences du contrôle* a posteriori*, projet d'arrêté sur la rénovation de la preuve d'arrivée à destination et de l'acquit à caution, projets de loi sur les embargos et l'intermédiation, arrêté sur la prolongation de la durée de la certification des entreprises.*

[3] *Actualisation de la « liste des matériels de guerre et matériels assimilés » - Arrêté de classement du 16 mars 2015 modifiant l'arrêté du 27 juin 2012.*

certifiées, ainsi que ceux destinés à élaborer une définition des matériels spécialement conçus pour un usage militaire, dont l'objectif final est de faciliter les procédures de classement des matériels de guerre pour les industriels.

Il participe activement aux travaux internationaux sur les matériels de guerre et anime le sous-comité de l'accord-cadre « Lettre d'intention »[1], chargé notamment de la simplification des procédures applicables aux transferts entre les six pays membres[2].

La commission dite « de l'article 90 »[3], présidée par le SGDSN, s'est réunie six fois entre juin 2015 et juin 2016. Sur cette période, et sur les sept nouvelles opérations présentées à la commission, six ont fait l'objet d'un avis favorable pour l'octroi d'une avance remboursable pour un montant total d'environ 40 M€. Actuellement, 68 programmes sont en cours d'exécution pour 38 entreprises pour un volume d'encours de plus de 95 M€ au 31 décembre 2015. Compte tenu de son caractère autofinancé, le dispositif de « l'article 90 » a fait l'objet d'une revitalisation récente dans une double direction : les PME/ETI d'une part et les grands groupes industriels agissant sur des projets stratégiques dédiés à l'exportation, d'autre part.

Il participe, en outre, aux travaux internationaux sur les biens à double usage[4].

---

[1] *La* Letter of Intent *(LoI) a été signée par les ministres de la défense des six pays principaux producteurs d'armement en Europe (Allemagne, Espagne, France, Italie, Royaume-Uni, Suède). Ces derniers mois, les efforts ont porté, conjointement avec les partenaires sur l'harmonisation du contenu des licences générales de transfert.*

[2] *Il a permis l'adoption, début 2016, d'un second « papier de position » commune avec des recommandations servant 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 fin 2016).*

[3] *La procédure dite de « l'Article 90 » permet à l'État d'octroyer des avances remboursables aux entreprises du secteur de la défense pour financer jusqu'à 50 % des dépenses d'industrialisation de produits militaires en vue de leur exportation. L'adaptation de leur gamme de produit à l'export permet aux entreprises de diversifier leurs débouchés commerciaux et de maintenir/développer des compétences au sein de la Base Industrielle et Technologique de Défense. Ces avances remboursables constituent une pièce essentielle et autofinancée du dispositif de soutien aux exportations de défense qu'il est opportun de pérenniser dans sa forme actuelle, car il donne entière satisfaction aux entreprises, renforce la compétitivité de la France à l'international et fonctionne sans coût pour l'Etat. En effet, outre la pérennisation de l'outil industriel et, avec elle, l'indépendance technologique et stratégique de la France, les remboursements et les redevances acquis grâce aux contrats en faveur des industriels contribuent à assurer l'équilibre de la procédure, et donc son autofinancement.*

[4] *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. Le président de la commission interministérielle des biens à double usage (CIBDU) sollicite le SGDSN, membre de la CIBDU, pour conduire l'instruction de dossiers particulièrement sensibles (pour des motifs techniques, politiques, en raison de l'impact sur l'emploi ou le tissu industriel local, etc.), dans un contexte interministériel adapté.*

L'année 2017 sera marquée par la poursuite des travaux de transposition. De nouveaux chantiers européens seront ouverts pour faciliter les transferts de données – y compris sensibles – entre les filiales européennes d'un même groupe (AIRBUS, MBDA, KNDS). En outre, une nouvelle licence générale sur les transferts de technologies sera négociée à Bruxelles. La facilitation de ces échanges contribuera à améliorer la compétitivité des entreprises et facilitera le développement de programmes industriels conjoints.

C'est aussi à ce titre que le SGDSN a été amené à suivre les dossiers industriels sensibles comme, en 2015, 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.

B. 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) 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[1]**, 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 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.

---

[1] 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.*

1. 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] a fait l'objet d'un processus d'évaluation après un an de mise en œuvre et dans le contexte *post* attentats de janvier 2015.

En s'appuyant sur le retour d'expérience des crises terroristes que la France a connues en 2015 et 2016, ainsi que sur les nouvelles dispositions législatives adoptées en 2016, le SGDSN a procédé à la rénovation du plan publié en janvier 2014. Des améliorations sensibles y ont été apportées, notamment en adaptant les niveaux de postures au niveau de la menace. Ainsi, en 2015, le SGDSN a diffusé, sur décision du Premier ministre, vingt-six postures « VIGIPIRATE ». En 2016, cinq postures ont été diffusées. La première l'a été en janvier. La deuxième a été diffusée en mars après les attentats de Bruxelles. La troisième a été diffusée en juin, afin de prendre en compte l'organisation du championnat d'Europe de football 2016. La quatrième a été diffusée en juillet, après l'attentat de Nice. Enfin, la cinquième posture, dite « posture de rentrée » a été diffusée en septembre.

Cette rénovation a été accompagnée d'un accroissement significatif de la sensibilisation à la menace terroriste, par la diffusion, vers un public élargi, d'une culture de la vigilance et de la conduite à tenir en cas d'attentat[2].

Le SGDSN a par ailleurs diffusé, pour le championnat d'Europe de football 2016, une version provisoire des plans « PIRANET » et « NRBC », en cours d'actualisation. Les versions définitives des plans seront achevées d'ici la fin de l'année et seront testées à l'occasion d'exercices majeurs.

La révision du plan « PIRATE-MER » a été engagée conjointement avec le secrétariat général de la mer, conformément à la stratégie nationale de sûreté des espaces maritimes approuvée par le Premier ministre le 22 octobre 2015. Elle s'appuie sur une nouvelle évaluation des menaces maritimes diffusée en juillet 2016. Le nouveau plan devrait être disponible à la fin de l'année 2016 pour être testé lors d'un exercice majeur en 2017.

---

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

[2] *Durant l'année 2016, 11 guides de bonnes pratiques ont été conçus par le SGDSN et réalisés conjointement avec le service d'information du Gouvernement et les ministères. Ces documents visent à renforcer la protection de certains bâtiments, établissements ou sites sensibles. Ils ont été largement diffusés pendant l'année 2016 vers les établissements scolaires, les centres commerciaux, les musées, les salles de spectacle, et à l'usage des maires. D'autres guides sont en cours de finalisation (hôpitaux, parcs de loisir, événementiel, universités, affaires étrangères, espaces de bureaux). Ce travail sera poursuivi en 2017.*

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

L'État organise et met 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 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 auprès de deux zones de défense et de sécurité pilotes (Île-de-France et Sud-Est). Elle associe, plus étroitement qu'auparavant, l'ensemble des acteurs territoriaux de la préparation et de la gestion des crises, en particulier les collectivités territoriales et opérateurs économiques, et vise à assurer une parfaite cohérence entre la planification gouvernementale ou locale et les capacités territoriales.

Les travaux du CGI se sont accélérés en 2016 en tenant compte, d'une part, du retour d'expérience des crises terroristes et, d'autre part, de la préparation du championnat d'Europe de football. Dans le cadre du Pacte de sécurité, le SGDSN a financé, pour le compte du ministère des affaires sociales et de la santé, l'achat d'équipements NRBC destinés aux services d'aide médicale urgente (SAMU) pour la prise en charge des victimes les plus gravement atteintes (2,8 M€). Cet effort financier sera renouvelé en 2017.

Conformément aux dispositions définies dans le CGI, le SGDSN tiendra une réunion interministérielle à la fin de l'année 2016 pour analyser les engagements financiers déjà réalisés par les ministères et ceux qui sont envisagés en 2017. L'analyse de risque portera sur la capacité d'anticipation de l'État. Cette démarche a permis de mieux appréhender l'évaluation de la menace dans le dispositif du nouveau plan « VIGIPIRATE » et de mieux délimiter les capacités essentielles à la résilience de la nation[1].

La gestion des crises majeures comporte une dimension internationale. Le SGDSN soutient le Secrétariat général des affaires européennes pour la mise en œuvre de la stratégie de sécurité intérieure de

[1] *Voir supra p.21*

l'UE. Par ailleurs, il a poursuivi, en lien avec le coordonnateur national du renseignement et les ministères concernés, ses actions de coopération dans le domaine de la prévention et de la lutte contre le terrorisme, en particulier avec le Royaume-Uni, les États-Unis d'Amérique et la République Fédérale d'Allemagne. A la suite des événements survenus en 2015, en France et en Belgique, il a développé une relation étroite avec ses homologues belges par l'échange d'éléments de posture.

En 2017, la circulaire du 2 janvier 2012 relative à l'organisation gouvernementale pour la gestion des crises majeures sera révisée pour prendre en compte la place prise par les conseils de défense et de sécurité nationale dans le dispositif de gestion politique et stratégique du temps de crise.

Le travail prospectif réalisé par le SGDSN sur la conduite à tenir en cas de multi-attentats, utilisé notamment au moment des attentats du 13 novembre 2015, sera prolongé pour en assurer une déclinaison territoriale.

Par ailleurs, la création du contrat général interministériel, fixant les « capacités-pivots » nécessaires aux ministères pour faire face aux risques et aux menaces, a mis en lumière une faiblesse du volet logistique associé à ces capacités, susceptible de fragiliser les pouvoirs publics en cas de crise grave. Face à ce constat, le cabinet du Premier ministre a confié un mandat au SGDSN pour étudier la mise en place d'un dispositif logistique interministériel associant l'ensemble des moyens publics et privés. Initiés en 2016, ces travaux seront finalisés pour l'année 2017.

3. La consolidation d'une filière industrielle française de sécurité

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. Depuis son installation par le Premier ministre le 23 octobre 2013, le CoFIS promeut la compétitivité de la filière.

[1] *Le Livre blanc de 2013 s'inspirait des recommandations de votre commission dans son rapport d'information sur la cyberdéfense de juillet 2012, « 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*

Les activités du CoFIS

Le CoFIS s'articule avec les plans de la « Nouvelle France Industrielle » et la stratégie nationale de recherche. S'agissant d'un secteur sensible au plan stratégique (la garantie de l'autonomie nationale dans les secteurs les plus sensibles) et au plan sociétal (la combinaison de la sécurité et du respect des libertés individuelles), son pilotage est effectué par le Premier ministre.

Depuis janvier 2014, une étude du marché national de la sécurité a permis de mieux connaître ses acteurs et son poids économique évalué à 30 milliards d'euros et 300 000 emplois dans le secteur marchand. Plusieurs projets structurants de démonstrateurs ont été lancés dans les secteurs clefs.

Le deuxième comité directeur du CoFIS, tenu le 1er décembre 2015 (…), a approuvé la feuille de route 2016-2017 structurée autour de quatre axes principaux : fédérer et valoriser tous les acteurs de la filière, en particulier les PME et les acteurs locaux, développer une offre innovante et adaptée, développer la base industrielle de sécurité, accéder au marché national et à l'export.

Dans ce cadre, il a organisé en septembre 2016, les premières assises de la filière des industries de sécurité.

Le SGDSN continuera en 2017 à participer au financement des projets de sécurité et de cybersécurité auprès de l'Agence nationale de la recherche (ANR) et du fonds unique interministériel (FUI). De même, il participera au financement de nouvelles solutions de lutte contre les menaces nucléaires, radiologiques, biologiques, chimiques et explosives. Enfin, il poursuivra son action de promotion des intérêts français dans le cadre du programme européen « Horizon 2020 ».

Source : SGDSN - Réponses au questionnaire parlementaire

Par ailleurs, le commissariat général à l'investissement a retenu la sécurité comme l'un des axes du troisième volet du plan d'investissement d'avenir. Ce volet devrait permettre de consacrer 10 milliards d'euros à la préparation de l'avenir. A ce jour, il existe une forme de consensus au sein de la filière des industries de sécurité pour considérer qu'un investissement de 900 M€ en trois ans dans le domaine des industries de sécurité aurait un effet hautement structurant.

Dans un souci d'efficacité dans l'affectation de ces nouveaux moyens au bénéfice de la filière, vos rapporteurs considèrent que le renforcement de l'organisation interministérielle accompagnant la structuration de cette filière est nécessaire.

4. Le renforcement des politiques de protection contre les menaces et risques majeurs

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

Face à une menace terroriste particulièrement élevée, la mission de protection « SENTINELLE » concrétise, depuis le mois de janvier 2015, le déploiement durable des armées sur le territoire national. Dans ce contexte, 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. Cette demande s'est traduite par la remise au Premier ministre du rapport relatif à l'engagement des armées sur le territoire national, le 17 février 2016.

Fondés sur le retour d'expérience, ces travaux ont permis d'identifier des évolutions souhaitables à court et moyen termes. Les modes d'action, le partage des prérogatives et des responsabilités entre forces militaires du ministère de la défense et forces du ministère de l'intérieur, ainsi que la coordination militaire, ont notamment été étudiés. Cette réflexion a permis la remise en perspective du rôle des armées dans la protection du territoire national. Ces travaux ont précédé la présentation aux assemblées parlementaires d'un rapport du Gouvernement sur les conditions d'emploi des armées lorsqu'elles interviennent sur le territoire national pour protéger les populations[1]. Ce rapport a fait l'objet d'un débat au Parlement[2], les 15 et 16 mars. Les mesures préconisées dans ce rapport sont mises en œuvre pour celles qui relèvent d'aspects purement opérationnels, ou en cours de prise en compte pour celles qui nécessitent des adaptations d'ordre juridique ou doctrinal. Parallèlement, le Parlement a conduit des travaux sur la présence et l'emploi des forces armées sur le territoire national[3] et sur la garde nationale[4]. De son côté, le SGDSN a engagé, au niveau interministériel, depuis le mois de juillet 2016, une révision de l'instruction interministérielle 10100 relative à l'engagement des armées sur le théâtre national en cas de crise majeure. Cette révision se conclura au début de l'année 2017.

b) 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), qui concernent les secteurs de résilience de la nation, se poursuit. Elle 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'Agence nationale de la sécurité des systèmes d'information (ANSSI). En 2015, six DNS ainsi rénovées ont été approuvées. Elles portent respectivement sur les communications électroniques et internet, l'électricité, le gaz, les hydrocarbures, les produits

[1] *http://www.ihedn.fr/userfiles/file/debats_fond/discours%20&%20documents/Rapport%20emplois%20force%20arm%C3%83%C2%A9es.pdf*
[2] *https://www.senat.fr/cra/s20160315/s20160315_7.html*
[3] *Rapport d'information n° 3864 de MM. Olivier Audibert Troin et Christophe Léonard, députés, au nom de la commission de la défense nationale et des forces armées, 22 juin 2016* http://www.assemblee-nationale.fr/14/rap-info/i3864.asp
[4] *Rapport d'information n° 793 (2015-2016) de M. Jean-Marie Bockel et Mme Gisèle Jourda, sénateurs, au nom de la commission des affaires étrangères, de la défense et des forces armées – 13 juillet 2016 http://www.senat.fr/notice-rapport/2015/r15-793-notice.html*

de santé et le transport aérien. Dans le même temps, la révision de onze autres DNS a été engagée.

c) La protection des installations et des sites sensibles

A la suite des événements survenus en 2015 sur les sites industriels sensibles de Saint-Quentin-Fallavier et de Berre-l'Etang, le SGDSN a reçu du Premier ministre un mandat pour conduire des travaux interministériels visant à renforcer la sécurité de ces sites à l'égard des menaces malveillantes. Un bilan complet des actions menées en application de l'instruction du Gouvernement du 30 juillet 2015 relative au renforcement de la sécurité des sites classés « SEVESO » contre les actes de malveillance et le rapport final, objet d'un consensus interministériel, a été transmis au Premier ministre le 3 mai 2016. Il traite notamment des conditions d'intégration de 78[1] sites classés « SEVESO » dans le dispositif de SAIV et la possibilité de demander aux exploitants de réaliser des études de sûreté portant sur des scénarios de malveillance[2]. Par ailleurs, des travaux ont été engagés dans le cadre du comité de la filière industrielle de sécurité (CoFIS)[3] pour l'élaboration d'une offre de solutions technologiques adaptée à la sécurité des sites industriels sensibles.

S'agissant plus spécifiquement de la protection physique des installations nucléaires, le SGDSN a poursuivi la mise en œuvre des conclusions des travaux interministériels menés en 2014 et 2015. Ainsi, après la modification de la partie législative du code général des collectivités territoriales permettant aux préfets de réglementer la circulation et le stationnement aux abords des installations nucléaires, la loi n° 2015-588 du 2 juin 2015 relative au renforcement de la protection des installations civiles abritant des matières nucléaires[4], a permis de créer le délit d'intrusion dans une zone nucléaire à accès réglementé[5]. En application de l'article 2 de cette loi, un travail interministériel a été mené sous l'égide du SGDSN sur les risques et les menaces spécifiques que constituent les survols illégaux par des aéronefs télépilotés. Ce travail a mis en exergue un certain nombre de lacunes juridiques et capacitaires face aux usages malveillants ou accidentels de drones aériens civils et proposé plusieurs pistes d'amélioration dans ces

---

[1] *Parmi les quelque 1 200 sites classés « SEVESO ».*

[2] *Les principales recommandations du rapport de la mission interministérielle d'inspection sur la publication d'informations potentiellement sensibles relatives aux installations classées « SEVESO », remis en mars 2016, ont en outre été intégrées à la réflexion*

[3] *Voir supra p 24.*

[4] *Loi n° 2015-588 du 2 juin 2015 relative au renforcement de la protection des installations civiles abritant des matières nucléaires*
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030664022&dateTexte=20161021

[5] *Le décret n° 2015-1255 du 8 octobre 2015 précise les locaux et terrains clos concernés. A ce stade, vingt zones ont été délimitées par arrêtés du ministère de l'environnement, de l'énergie et de la mer.*
https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031288120&dateTexte=20161021

deux domaines, sans obérer le développement d'une filière créatrice d'emplois[1].

d) 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.

Le SGDSN produit également des analyses thématiques régulières à destination des autorités gouvernementales, en s'appuyant sur sa capacité de veille et d'alerte. C'est le cas notamment dans le domaine des explosifs[2] et dans le domaine NRBC[3], dans le secteur du transport aérien (v. encadré ci-dessous) et dans le domaine maritime[4].

Évaluation des risques dans le domaine aérien

Avec l'appui du pôle d'analyse du risque pour l'aviation civile (PARAC) de la direction générale de l'aviation civile (DGAC), le SGDSN a poursuivi, en lien avec les ministères concernés, la supervision des dispositifs permettant d'évaluer le risque pour les vols en provenance de pays jugés sensibles et de lutter contre la menace des missiles sol-air de très courte portée (« MANPADS »). Le programme d'évaluation des escales sensibles a été renforcé, conformément aux décisions prises lors de la commission interministérielle de la sûreté aérienne (CISA) qui s'est tenue en avril 2016, tandis que le programme de lutte contre la menace MANPADS a été étendu aux plateformes aéroportuaires nationales. Ces différents programmes mettent également à contribution les partenariats internationaux noués avec nos plus proches alliés, en particulier la Grande-Bretagne et les États-Unis.

[1] *Voir supra p.25*

[2] *Le SGDSN identifie, avec l'aide des services de renseignement, les explosifs pouvant être mis en œuvre par des groupes terroristes. Il finance également des travaux de caractérisation des explosifs afin d'identifier si les nouvelles matières, retrouvées notamment sur les théâtres extérieurs et susceptibles d'être utilisées en France, sont dangereuses ou non. Une fois la liste des matières explosives établie, le SGDSN en vérifie la pertinence et préconise les mesures de prévention, de détection et de protection à déployer. Si des lacunes sont identifiées, le SGDSN oriente et, le cas échéant, finance des actions de recherche et de développement, notamment en matière de technologies de détection.*

[3] *L'analyse des risques s'est appuyée sur l'élaboration en 2014 d'une dizaine de* scénarii *de référence qui ont été actualisés, notamment dans la perspective du championnat d'Europe de football et de la rénovation du plan NRBC, en cours de finalisation, et qui servent de base au perfectionnement du dispositif de réponse dans le cadre du comité stratégique NRBC-E, présidé par le SGDSN.*

[4] *Le SGDSN, en lien avec le coordonnateur national du renseignement (CNR) et les services de renseignement, a élaboré une évaluation des menaces, conformément au plan d'actions pour la mise en œuvre de la stratégie nationale de sûreté des espaces maritimes.*

Le 20 octobre 2015, après un an de travaux interministériels et en application de l'article 2 de la loi n° 2015-588 du 2 juin 2015 relative au renforcement de la protection des installations civiles abritant des matières nucléaires, le SGDSN a remis au Parlement un rapport intitulé « L'essor des drones aériens civils en France : enjeux et réponses possibles de l'État ». Le rapport suggère des orientations qui ont ensuite été développées en 2016 :

- adapter et compléter le corpus juridique existant en instaurant un nombre limité de nouvelles obligations, notamment dans les domaines de l'information, de la formation, de l'immatriculation et de l'identification : **la proposition de loi relative au renforcement de la sécurité de l'usage des drones civils, déposée par nos collègues Xavier Pintat et Jacques Gautier[1] a été définitivement adoptée par le Sénat le 13 octobre 2016**;

- accélérer les travaux de recherche et de développement, y compris dans le cadre de coopérations bilatérales et multilatérales : le développement accéléré de trois projets de démonstrateurs de contre-mesures anti-drones, financé par le SGDSN et conduit en partenariat avec l'Agence nationale de la recherche (ANR), doit aboutir en 2016 ;

- disposer au plus vite de moyens efficaces de détection, d'identification et de neutralisation des drones de petites dimensions : des dispositifs intérimaires de lutte anti-drones ont notamment été déployés tout au long du championnat d'Europe de football.

e) Le renforcement de la résilience et de la continuité des activités essentielles de la Nation

Le SGDSN, pilote de la démarche nationale de résilience, a mené et soutenu en 2016 de nombreux projets dans ce cadre, essentiellement autour des axes « information et sensibilisation des parties prenantes à la stratégie de sécurité nationale » et « continuité des activités essentielles de la Nation ».

L'effort accru de sensibilisation à la menace terroriste[2] fait partie des actions menées par le SGDSN[3].

L'action de résilience passe par l'organisation d'exercices majeurs. Deux exercices ont été organisés en 2016.

En mars dernier, le SGDSN a organisé l'exercice gouvernemental « CRUE DE SEINE 2016 », en l'articulant avec l'exercice de la zone de défense et de sécurité de Paris « EU SEQUANA 16 » afin de tester le plan de continuité du travail gouvernemental en cas de crue majeure de la Seine et de permettre aux ministères de mettre en œuvre tout ou partie de leurs plans d'opérations.

L'exercice « SECNUC16 », joué en septembre, a permis de tester un scénario de catastrophe industrielle dans le domaine nucléaire. En 2017, trois exercices seront organisés. Ils porteront sur les questions de contre-terrorisme maritime, de sécurité des transports et de danger NRBC.

---

[1] http://www.senat.fr/dossier-legislatif/ppl15-504.html

[2] *voir supra p.21*

[3] *Le lancement par le ministère de l'intérieur et le service d'information du Gouvernement de l'application ordiphone « SAIP » le 7 juin dernier participe également de cette politique de promotion et de mise au point des outils d'alerte et d'information des populations.*

f) L'amélioration de la protection de l'information et la consolidation de la protection générale des dispositifs de sécurité.

Le développement des inspections portant sur le respect des règles de protection des informations classifiées « Très Secret », dont le SGDSN a la pleine responsabilité, a été poursuivi avec dix-neuf inspections menées au cours de l'année écoulée, sur des sites de l'État comme de certaines entreprises.

Pour la première fois, le SGDSN a élaboré et publié un rapport sur le secret de la défense nationale en France en 2015[1]. Le secrétariat général est en effet chargé de concevoir et de faire respecter les mesures de protection de ce secret. Ce rapport présente les explications et les données statistiques sur le secret de la défense nationale.

Une révision sensible de l'instruction générale interministérielle n° 1300 du 30 novembre 2011 sur la protection du secret de la défense nationale, qui organise la protection du secret en France, est en cours pour mieux intégrer la dématérialisation des données dans la réglementation relative aux informations classifiées et mettre en adéquation le droit et les pratiques avec ceux de nos principaux partenaires étrangers. Le projet d'instruction générale interministérielle n° 1300 sur la protection du secret, en cours de validation, pourrait entrer en vigueur courant 2017.

Vos rapporteurs saluent cet effort. Ils estiment que des progrès doivent être réalisés dans la connaissance des règles du secret de la défense nationale et des procédures de mise en œuvre et souhaitent qu'un effort de formation continue soit engagé en direction des administrations et des entreprises des secteurs sensibles, mais également qu'une formation initiale soit donnée dans les écoles d'ingénieurs et dans les écoles de formation des futurs cadres des entreprises (école de commerce et de gestion) et des administrations (ENA, IRA…).

Par ailleurs, des négociations ont été lancées en vue de la signature d'accords généraux de sécurité (AGS) avec le Canada, l'Australie et Israël. Des discussions sont également engagées pour l'actualisation des accords liant la France à la Belgique et à la Norvège.

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

Le secrétaire général de la défense et de la sécurité nationale a la mission de proposer au Premier ministre et de mettre en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information[2]. Il

[1] http://www.sgdsn.gouv.fr/IMG/pdf/2015-12-16_RAPPORT_SUR_LE_SECRET_DE_LA_DEFENSE_NATIONALE_EN_FRANCE.pdf

[2] *Article R.132-3 du code de la défense,*

dispose à cette fin d'un service à compétence nationale « Agence nationale de la sécurité des systèmes d'information (ANSSI) » dont les missions sont définies par le décret n° 2009-834 du 7 juillet 2009 modifié[1] notamment en 2015 pour tenir compte des évolutions portées par les dispositions de la loi de programmation militaire de décembre 2013.

Le secrétaire général de la défense et de la sécurité nationale fixe annuellement un contrat d'objectifs au directeur général de l'ANSSI. Il valide la stratégie de l'agence. Il en suit l'activité. 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.

Les missions de l'agence s'organisent autour de deux pôles :

- un pôle de sensibilisation et de prévention, destiné à informer les acteurs publics des menaces présentes dans le cyberespace et des moyens de s'en protéger. Ce pôle 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 ;

- un pôle de réaction aux attaques, dans lequel le centre opérationnel de la sécurité des systèmes d'information (COSSI) assure la réponse de l'État en termes de défense.

L'actualité opérationnelle de l'agence entraîne un élargissement et une redéfinition, bien engagée, de ses missions. Le rapport d'activité 2015 de l'ANSSI, donne une vision détaillée des missions actuelles et à court terme[2].

A. LA CYBERDÉFENSE RESTE UNE PRIORITÉ NATIONALE

1. Une menace qui ne cesse de s'accroître

Comme le rappelait son directeur général devant votre commission[3], **l'étendue de la menace ne cesse de s'accroître**. « *Dans le domaine de la cybersécurité, les menaces sont polymorphes du fait du développement du numérique. Les industries et les États sont les cibles prioritaires. Le phénomène est inquiétant. Cette menace rapporte plusieurs milliards d'euros aux groupes qui agissent souvent loin du territoire national. C'est une menace qui (…) a des*

[1] *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000020828572&dateTexte=20161115*
[2] *https://www.ssi.gouv.fr/actualite/rapport-dactivite-de-lanssi-2015-une-annee-charniere-pour-la-concretisation-des-actions-engagees/*
[3] *http://www.senat.fr/compte-rendu-commissions/20161017/etr.html#toc4*

conséquences sur la disponibilité des services, la compétitivité des entreprises et peut provoquer des pertes de vies humaines.

La déstabilisation des systèmes informatiques nécessaires au fonctionnement de nombre de services publics tels que les hôpitaux ou la distribution d'électricité est une forme nouvelle de menace. Comme l'a montré l'actualité récente des élections américaines, des partis politiques sont également ciblés par des actes de piratages…

Nos deux inquiétudes principales (…) concernent en premier lieu le vol d'informations et de données qui est quotidien. Ainsi, 20 attaques majeures à des fins d'espionnage ont été subies par des grandes entreprises françaises au cours de l'année, ce qui représente des pertes économiques et stratégiques lourdes (vols de brevets, courriels, appels d'offres, données financières et commerciales). (…). Le deuxième risque est celui du sabotage informatique qui peut causer des pertes de vies humaines lorsqu'il vise des systèmes d'information de services publics (aiguillages ferroviaires, contrôle aérien, équipement hospitalier) ».

2. La France est classée désormais au 9e rang mondial des pays où la cybercriminalité est la plus active

Le rapport Symantec 2016 met en avant l'organisation toujours plus efficace des cybercriminels. Aujourd'hui, ces derniers adoptent les pratiques du monde professionnel et créent donc de véritables structures pour qu'ils gagnent en efficacité. Bien évidemment, cette organisation explique aussi la multiplication des actions menées par les pirates au cours de l'année 2015. Ce sont d'ailleurs 430 millions de variantes de programmes malveillants qui sont apparus sur le marché au cours de la dernière année, preuve que la cybercriminalité progresse.

Autres sources d'inquiétudes, les grands groupes cybercriminels ont pris une ampleur telle qu'ils sont devenus à la fois exécutants pour exploiter certaines failles mais aussi vendeurs de solutions de *hacking* à des petits escrocs voulant se faire une place dans ce business fort rentable.

Les données rassemblées par Symantec dans le rapport *Internet Security Threat Report* (ISTR) mettent en avant six découvertes et tendances marquantes de l'année 2015.

En moyenne, une nouvelle vulnérabilité *Zero Day* a été découverte par semaine. Les attaquants les plus dangereux continuent de se servir des défauts présents sur les navigateurs et *plug-ins* de sites web. Au niveau mondial, les vulnérabilités « zero-day », c'est-à-dire qui utilisent des failles non détectées jusque-là dans un logiciel, ont été multipliées par deux par rapport à 2014 pour atteindre un nombre record de 54 découvertes.

Un demi-milliard de dossiers personnels ont été volés ou perdus. Le nombre d'entreprises ne signalant pas la réelle portée des violations de données dont elles ont été victimes est plus élevé que jamais.

Trois quarts des sites Web populaires contiennent des vulnérabilités majeures en termes de sécurité. Les administrateurs Web peinent à développer des correctifs à temps.

Le nombre de campagnes d'hameçonnage ciblant les employés a augmenté de 55 %. Les attaquants jouent la carte de la patience avec les grandes entreprises.

Le nombre de *ransomwares* a augmenté de 35 %. Les cybercriminels utilisent le chiffrement comme une arme pour prendre les données essentielles des particuliers et des entreprises en otage.

Cent millions de fraudes au support technique ont été bloquées. Les pirates à l'origine des fraudes vous obligent maintenant à les appeler pour vous rendre votre argent.

La France est passée en un an de la 14e à la 9e place du classement des pays où la cybercriminalité est la plus active qui reste dominé par le même podium, avec la Chine, les États-Unis et l'Inde.

Cette remontée est en particulier due à une nouvelle hausse des « *rançongiciels* », qui ont représenté plus de 391 000 attaques en France en 2015, soit 2,6 fois plus qu'un an plus tôt, qui consiste à chiffrer les données du site attaqué et à délivrer contre rançon la clef de déchiffrement. Les attaques contre les administrations publiques, notamment les hôpitaux, se sont multipliées.

Les arnaques sur les réseaux sociaux ont également fortement augmenté durant l'année écoulée, un domaine où la France se classe 2e en Europe et 4e au niveau mondial, avec pas moins de 300 000 arnaques détectées.

Sources :
Symantec https://www.symantec.com/fr/fr/security_response/publications/threatreport.jsp
Le Parisien - 12 avril 2016
DGRIS Observatoire du monde cybernétique – lettre n° 49 avril 2016

3. La montée en puissance des agences de cyberdéfense

Face à cette menace qui va continuer à se développer, l'ANSSI va poursuivre sa montée en puissance. Le Royaume-Uni et l'Allemagne s'inscrivent dans la même démarche. Les Britanniques sont en train d'ouvrir leur centre national de cybersécurité doté d'emblée de 700 personnes et le BSI allemand, qui dépend du ministère de l'intérieur et emploie 600 personnes, annonce le recrutement de 180 salariés supplémentaires en 2017, de manière à répondre à l'accroissement des missions.

B. UNE DÉMARCHE STRATÉGIQUE ENGAGÉE POUR FAIRE FACE À CETTE MENACE

Cette démarche a été engagée par le Livre blanc sur la défense et la sécurité nationale et affermie par la loi de programmation militaire (LPM) 2014-2019 du 18 décembre 2013 qui a confié de nouvelles missions à l'ANSSI. Elle a été prolongée par la stratégie nationale pour la sécurité numérique, présentée en juin 2015, pour accompagner la transition numérique en assurant la protection des systèmes liés aux intérêts nationaux et enfin la stratégie nationale de sécurité du numérique présentée en octobre 2015.

1. La LPM 2014-2019 : une nouvelle étape dans la prise en compte par les pouvoirs publics des questions liées à la cybersécurité

Des dispositions législatives ont été introduites par la loi de programmation militaire du 18 décembre 2013[1] pour conforter le cadre juridique de l'action de l'Etat.

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.**

La LPM répond également à la hausse prévisible de la demande d'audits de sécurité, en encadrant la définition de prestataires d'audits de systèmes de sécurité informatiques de confiance. LPM confie à l'ANSSI de nouvelles missions, notamment en matière de protection des systèmes d'information critiques des opérateurs d'importance vitale.

2. 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.

3. La stratégie nationale de sécurité du numérique

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.[2]

En conformité avec la stratégie nationale pour la sécurité du numérique, cinq axes vont concentrer l'action de l'ANSSI sur la période 2016– 2017 :

- la généralisation des usages du numérique : des secteurs d'activité ou des collectivités locales, jusque-là peu numérisés, rattrapent leur retard et

---

[1] *Rapport pour avis n° 166 - Tome IX (2015-2016) de MM. Jean-Marie Bockel et Jean-Pierre Masseret, sénateurs, au nom de la commission des affaires étrangères, de la défense et des forces armées – 19 novembre 2015 - p.29* http://www.senat.fr/rap/a15-166-9/a15-166-9.html

[2] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf

devront être accompagnés sur le plan de la sécurité. Cela se traduira pour l'ANSSI par la nécessité de disposer de relais dans ces secteurs ;

- la publication des premiers arrêtés d'application de l'article 22 de la LPM en 2016 conduit l'ANSSI à accroître son assistance aux opérateurs d'importance vitale. Cet élargissement conduira à renforcer les structures de coordination, de conseil, mais également de contrôle et d'assistance opérationnelle ;

- la prise de conscience des enjeux liés à la sécurité du numérique conduit les ministères comme les entreprises à exprimer un besoin croissant de sécurité ; pour l'ANSSI, cela se traduit par une augmentation du nombre de produits et services soumis à qualification ou à certification ;

- la mise en œuvre de moyens techniques plus sophistiqués, en réponse à une complexité et volume des opérations de cyberdéfense croissants ;

- le renforcement de l'influence de l'ANSSI dans le cadre d'une coopération internationale.

4. Les travaux d'anticipation stratégique

Dans le prolongement de la stratégie nationale pour la sécurité du numérique, les travaux d'anticipation stratégique ont essentiellement porté sur l'élaboration de la stratégie de l'ANSSI pour la période 2016-2020. L'un des axes retenus, intitulé « connaissance et anticipation » a précisément pour objectif de renforcer la capacité de l'agence à anticiper les nouvelles menaces et à favoriser l'émergence de nouvelles technologies ou de nouveaux usages susceptibles d'avoir un impact en matière de sécurité informatique.

Parallèlement, l'ANSSI a contribué aux réflexions prospectives engagées par le SGDSN et, par exemple, proposé d'étudier l'impact que pourrait avoir le traitement massif de données pour l'élaboration de politiques de sécurité préventives ou encore de renforcer l'efficacité des politiques existantes. Une réflexion interministérielle est engagée en ce sens.

Conformément à l'une des orientations proposées par la stratégie nationale, l'ANSSI a par ailleurs proposé l'organisation d'une conférence internationale visant à donner une meilleure visibilité aux positions de la France en matière de construction de la paix par le droit dans un monde en transition numérique. Cette conférence devrait avoir lieu en avril 2017.

L'ANSSI a également participé à de nombreux travaux de prospective engagés par d'autres administrations ou autorités indépendantes. Ainsi, a-t-elle contribué à l'étude menée par l'ARCEP sur les objets connectés. **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.

Enfin, pour répondre à l'évolution du contexte de sécurité du numérique et à sa pénétration croissante dans tous les aspects de la vie de la nation, l'agence élabore des propositions susceptibles d'améliorer la sécurité des projets informatiques des administrations afin de les intégrer dans les travaux qui seront engagés à l'occasion du futur Livre blanc sur la défense et la sécurité nationale.

C. UNE CAPACITÉ D'EXPERTISE DE TRÈS HAUT NIVEAU

Six laboratoires, intégrés à la sous-direction Expertise, concentrent l'essentiel des activités de recherche de l'agence. Leurs domaines de compétence se répartissent entre la cryptographie, la sécurité des composants, la sécurité des technologies sans fil, les architectures matérielles et logicielles, les réseaux et protocoles, et les techniques de détection d'attaques. Ces structures aux rôles multiples sont à l'origine des référentiels techniques utilisés par l'ANSSI, et constituent donc un rouage essentiel des mécanismes d'évaluation, de labellisation et d'audit mis en œuvre par l'agence. L'élaboration de ces référentiels techniques est éclairée par le contact avec des infrastructures opérationnelles.

Ces laboratoires peuvent également contribuer à la création de produits sécurisés, à l'instar du laboratoire architectures matérielles et logicielles (LAM), et donnent lieu à des contacts suivis avec des acteurs industriels, mais aussi avec des utilisateurs, administrations ou opérateurs d'importance vitale (OIV).

L'ANSSI veille à appuyer ses recherches sur les avancées enregistrées par le monde scientifique académique.

> À cet égard, la création en 2015 du laboratoire exploration et recherche en détection (LED) est représentative de la stratégie de l'agence en la matière. Ce laboratoire, dont l'activité est dédiée à la problématique de la détection d'attaques, mène des travaux de recherche en collaboration avec l'École normale supérieure (ENS) et l'Inria, comme avec les équipes internes de l'agence.

Les travaux menés en son sein font régulièrement l'objet de publications à l'occasion de conférences scientifiques nationales et internationales. Ainsi, en 2015, pas moins de 40 publications ont vu le jour. Les compétences portées par les laboratoires de l'ANSSI lui permettent de s'affirmer comme un acteur crédible au niveau international.

D. LES ACTIONS DE L'ANSSI VERS LES ADMINISTRATIONS

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, en partenariat étroit avec le Centre de transmission gouvernemental (CTG) de développer, de déployer et d'assurer le support technique de systèmes de téléphones fixes (TEOREM), de visio-conférence (HORUS) ou d'intranet (ISIS).

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. Parallèlement à l'élargissement de son emploi par les services de l'État, y compris hors situations de crise, ce système a remplacé la messagerie sécurisée qui équipait les préfectures. Cela s'est traduit par une densification importante du réseau, avec le déploiement de 500 terminaux supplémentaires, portant leur nombre total à 1 350.

Vos rapporteurs s'interrogent 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 nécessaires à l'information des commissions parlementaires.

En parallèle de ses efforts en développement de technologies propres, l'agence cherche également à explorer de nouvelles approches en matière de fourniture de solutions sécurisées aux pouvoirs publics. Cette philosophie a présidé au lancement de projets portant sur l'exploitation de smartphones et tablettes disponibles dans le commerce, dans le souci permanent de privilégier l'ergonomie. Ainsi, en 2015, un système sécurisé fondé sur l'architecture Android, a été porté sur certains téléphones et tablettes et expérimenté à grande échelle de ce système en collaboration avec la Police nationale et avec la Gendarmerie nationale.

De la même manière, l'ANSSI s'est pour la première fois portée acquéreur d'une licence globale pour l'utilisation, par les services de l'État, d'un ensemble de logiciels de sécurité qualifiés auprès de la société Prim'X[1]. Cette initiative inédite permet à la fois d'optimiser la dépense publique et d'inciter les administrations à utiliser des produits de confiance tout en facilitant leur déploiement.

[1] *Cette opération permet aux administrations de répondre à leurs besoins de sécurisation pour un coût de licence nul, ne laissant à leur charge que les frais de support.*

2. Une sensibilisation de l'ensemble du Gouvernement par circulaire du Premier ministre : la « PSSIE »

Le Premier ministre a publié en juillet 2014 une circulaire fixant les règles de protection des systèmes d'information des différents départements ministériels[1]. Ce document préparé par l'ANSSI fixe les contours d'une « *Politique de sécurité des systèmes d'information de l'État* » (PSSIE). 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.

La mise en conformité des ministères avec la PSSIE est en cours, sous le pilotage des services des hauts fonctionnaires de défense et de sécurité. L'ANSSI apporte son soutien à cette démarche, à travers notamment les inspections qu'elle conduit, des actions de sensibilisation et un accompagnement ciblé pour la mise en place de certaines mesures.

Deux ans après sa publication, la PSSIE a été adoptée par l'ensemble des ministères, qui l'ont pour la plupart prise en compte dans leur politique ministérielle. Le niveau effectif de conformité des systèmes d'information de l'État aux règles de la PSSIE s'est légèrement amélioré entre 2015 et 2016. Il est attendu que les plans d'action engagés par les différents ministères permettent des progrès significatifs dans l'année à venir, notamment en matière de gouvernance et de maîtrise des risques.

Une révision de la PSSIE et des indicateurs associés n'apparaît pas nécessaire à court terme, les ministères ayant la possibilité de déroger si nécessaire à certaines règles de la PSSIE. Une telle révision pourra être engagée à partir de 2017, sur la base des retours d'expérience relatifs à la mise en œuvre du document.

La sécurité des systèmes d'information devenant un enjeu essentiel, 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[2] :

- améliorer la maturité globale des différents départements ministériels en matière de SSI ;

---

[1] *N° 5725/SG du 17 juillet 2014.*

[2] *Pour les précisions méthodologiques voir PAP programme 129 http://www.performance-publique.budget.gouv.fr/sites/performance_publique/files/farandole/ressources/2017/pap/html/DBGPGMOBJINDPGM129.htm*

- 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.

INDICATEUR 6.1 mission

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

(du point de vue de l'usager)

	Unité	2014 Réalisation	2015 Réalisation	2016 Prévision PAP 2016	2016 Prévision actualisée	2017 Prévision	2017 Cible
Maturité globale en sécurité des systèmes d'information de l'Etat	note de 0 à 5	3,3	2,3	2,4	2,6	3,1	2,7
Niveau d'avancement des grands projets interministériels en matière de sécurité des systèmes d'information	%	80	83	87	88	90	89

La poursuite des plans d'actions ministériels, relatifs à la mise en œuvre des règles de la politique de sécurité des systèmes d'information de l'État (PSSIE) ainsi que la correction des vulnérabilités les plus sensibles constatées lors d'audits et d'inspections[1], permettent de revoir la prévision pour l'année 2016 du sous-indicateur 1 : « Maturité globale en sécurité des systèmes d'information de l'État » légèrement à la hausse. Cette amélioration devrait se poursuivre en 2017 par la mise en conformité de l'essentiel des ministères avec les dispositions de la PSSIE relatives à la gouvernance et à la maîtrise des risques. **Cette situation reste néanmoins insatisfaisante au regard des objectifs de conformité complète à la PSSIE.** Elle peut, comme en 2015, être expliquée par un manque de moyens budgétaires et humains en matière de sécurité des systèmes d'information, ainsi que par une prise de conscience encore insuffisante des autorités, utilisateurs et exploitants face aux enjeux de cybersécurité. Si les ministères ont, pour la plupart, engagé des plans d'action de mise en conformité avec la PSSIE, le succès de ces plans et le maintien dans le temps d'un niveau de sécurité satisfaisant nécessite la mise en place d'une gouvernance adéquate, assortie de moyens adaptés. Cet effort a d'ores et déjà été consenti par plusieurs ministères et il est attendu qu'il soit étendu à l'ensemble des ministères. L'ANSSI s'efforcera donc en 2017 de continuer les efforts entrepris afin d'améliorer la sécurité des systèmes d'information de l'État.

[1] *L'ANSSI mène régulièrement des audits de sécurité des systèmes d'information des services de l'État, soumis à des inspections cycliques réglementaires. Ainsi, chaque ministère doit, par exemple, se soumettre à une inspection, en principe tous les 3 à 4 ans, portant à la fois sur la sécurité des systèmes informatiques considérés comme prioritaires et sur l'identification d'axes d'amélioration adaptés. Ces audits peuvent également être sollicités par les administrations, notamment lors de la mise en œuvre de grands projets de systèmes d'information.*

Vos rapporteurs s'inquiètent de la lenteur du processus de mise en conformité des ministères avec les dispositions de la PSSIE, compte tenu des efforts déployés par l'ANSSI.

Concernant le niveau d'avancement des grands projets interministériels en matière de sécurité des systèmes d'information (sous-indicateur n° 2). L'aboutissement avant fin 2016 d'un projet relatif à un produit souverain (chiffreur PMPS) permettra d'améliorer la prévision 2016 et la prévision qu'au moins trois sondes commerciales soient qualifiées, permettant ainsi de gagner un point par rapport à la cible 2017 fixée en début de triennal, permet ainsi de gagner un point par rapport à la cible 2017 fixée en début de triennal.

En parallèle, **l'ANSSI a développé une offre de formation en direction des agents de l'Etat.**

Le Centre de formation à la sécurité des systèmes d'information (CFSSI) remplit tout d'abord l'une des tâches stratégiques de l'agence, à savoir la formation des agents de l'État en matière de cybersécurité et propose à un important catalogue de stages adaptés à la multiplicité des besoins et des profils. En 2015, 1 450 stagiaires ont participé aux 28 formations organisées par l'agence.

Par ailleurs, le CFSSI assure une formation longue d'expert en sécurité des systèmes d'information (ESSI). Étalée sur une durée de treize mois et sanctionnée par un titre de niveau I (bac +5), elle est inscrite au Répertoire national des certifications professionnelles (RNCP). En 2015, le titre d'expert a été attribué à 8 élèves au sein du CFSSI et, dans le cadre d'un partenariat, à 11 élèves de la voie d'approfondissement Sécurité des systèmes et réseaux, en formation d'ingénieur à Télécom Sud Paris. Le titre peut également être obtenu par le biais d'une validation des acquis de l'expérience (VAE).

3. La politique d'investissement de l'ANSSI

Dans le cadre de ses missions, l'ANSSI contribue au financement des besoins des administrations en produits et services de sécurité. Cette démarche regroupe deux volets :

- la conception et la réalisation des moyens de communications électroniques sécurisées utiles au Gouvernement et à la présidence de la République, qui représente une part importante du budget de l'agence et implique l'utilisation de décrets de transfert annuels entre programmes en lien avec la DGA ;

- l'évaluation et les recommandations de produits ou de services pour l'usage des administrations, ce qui implique de définir les exigences techniques, de développer les outils nécessaires à leur évaluation, de les suivre dans le temps et d'en promouvoir l'utilisation[1].

[1] *Dans ce cadre, l'acquisition de licences globales pour l'administration permet l'adoption rapide et massive de logiciels recommandés conduisant à une élévation significative du niveau de sécurité des*

L'ANSSI porte également la mission de définir, concevoir et de mettre en œuvre des systèmes d'informations en adéquation avec les besoins fonctionnels exprimés et les besoins de sécurité requis pour ces systèmes. Elle assure un rôle de direction des systèmes d'information (DSI) et des ministères dans le cadre des systèmes d'information interministériels sécurisés dont elle assure la maitrise d'œuvre. Elle est également en charge de la conception des systèmes d'information internes et externes vers les administrations. Elle assure enfin le soutien des infrastructures informatiques de production relevant de la DSI.

Un projet de « centre informatique interministériel de haute sécurité » permettra d'accompagner la montée en puissance de l'ANSSI à travers un outil informatique performant et fiable. L'ANSSI utilise des données en masse (*big data*) et collecte énormément d'informations qui sont très précieuses pour la connaissance des modalités d'attaques de systèmes d'information et la mise au point de mesures de détection et de protection. Ces données proviennent de victimes de cyberattaques, de victimes potentielles, d'opérateurs d'importance vitale. Elles ne peuvent être stockées sur des serveurs étrangers ou privés, et doivent être protégées dans une enceinte sécurisée. La construction de ce centre est donc indispensable. Le projet est conduit avec le ministère de l'intérieur, maître d'ouvrage de l'opération. Une convention-cadre pour la réalisation et l'exploitation de ce site, ainsi qu'une convention de réalisation, ont été signées le 9 juillet 2015 afin de préciser les modalités de conception, de construction et de financement conjoints. La durée d'exécution prévue des travaux est de 30 mois, soit une mise en service de l'installation programmée pour le second semestre 2018.

4. La mobilisation du ministère de la défense sur l'enjeu « cyber »

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[1]. 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. En outre, le ministère de la défense va accélérer la

différents ministères. Ces licences sont incluses dans les dépenses de l'ANSSI pour 2017 à 3,9 M€ en AE et 4,4 M€ en CP- voir infra p.76

[1] Les 6 priorités du « pacte défense Cyber », voir Rapport pour avis n° 166 Tome IX (2015-2016) de MM. Jean-Marie Bockel et Jean-Pierre Masseret, sénateurs, au nom de la commission des affaires étrangères, de la défense et des forces armées – 19 novembre 2015, p. 34 - http://www.senat.fr/rap/a15-166-9/a15-166-9.html .

sécurisation du réseau interne du ministère de la défense (Intradef : 150 000 postes utilisateurs).

L'ANSSI est étroitement associée aux quatre actions d'axe 4 du pacte tout comme elle entretient plus généralement des échanges réguliers avec le Pôle d'excellence en cyberdéfense (PEC).

La coopération entre l'ANSSI et le Pôle d'excellence de cyberdéfense

Ces liens transparaissent notamment dans la coordination des actions en matière de formation à la cyberdéfense et à la sécurité numérique. Ainsi, le PEC a été représenté et a intégré le fruit de ses travaux au sein du groupe de travail, instauré dans le cadre de la NFI, qui a élaboré le mécanisme de labellisation de formations « SecNumEdu »[1] et assure également, dans le même cadre le pilotage d'un autre groupe de travail, portant sur les plateformes de formation et d'entraînement à la cybersécurité, et participe à des travaux sur l'amélioration de l'attractivité de la filière pour les étudiants.

La coopération s'étend également aux actions menées conjointement par l'ANSSI et le PEC pour promouvoir le développement économique des acteurs nationaux de la sécurité du numérique. Ainsi, le PEC s'est fortement impliqué, notamment par la fourniture d'un référentiel, dans l'action NFI visant la création d'un observatoire national du marché de la sécurité numérique. Il a également piloté l'action visant à recenser les plateformes nationales de tests et de recherche & développement dans le domaine de la sécurité numérique, et plus généralement, été un acteur important dans la définition de la feuille de route de la solution « Confiance Numérique » de la NFI.

Plus récemment, la mise en place d'un partenariat public-privé « cyber » au niveau européen a naturellement amené le PEC et l'ANSSI à se concerter étroitement afin d'assurer la meilleure représentation des acteurs nationaux au sein des instances de gouvernance de ce partenariat.

Dans le cadre de ce pacte, l'agence est également impliquée fortement dans la planification et le jeu de l'exercice annuel « DEFNET », placé sous la responsabilité du ministère de la défense, ainsi que dans l'organisation et le jeu d'exercices nationaux et internationaux.

5. 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 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. 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] *Voir infra p.52*

Le réseau interministériel de l'Etat (RIE) constitue le support de l'ensemble des échanges interministériels. Il remplace progressivement, depuis 2013, les réseaux ministériels existants, représentant près de 17 000 sites au démarrage du projet, et permet une fluidification des échanges interministériels, en particulier pour les sites de l'administration territoriale de l'État, qui sont enfin raccordés sur un réseau commun. Il marque la première étape de la modernisation et de l'unification du système d'information de l'État. A fin juillet 2016, il est déployé sur plus de 11 500 sites en métropole et dans les DOM COM, et 400 000 agents de l'État accèdent à internet via les passerelles d'accès à internet du RIE.

Le service à compétence nationale (SCN), en charge de la gestion du RIE et des services associés, a été créé par voie d'arrêté le 17 décembre 2012. Rattaché au directeur interministériel du numérique et du système d'information et de communication de l'État, ce service s'appuie sur les instances de gouvernance de la DINSIC[1].

Le RIE : un investissement important

Le cadrage budgétaire initial du projet RIE, en 2012, repose sur un budget de fonctionnement annuel estimé pour 15 822 sites à 53,9 M€ à mettre en regard avec ce qu'aurait coûté le maintien à l'existant des réseaux ministériels sans le projet RIE, 72,1 M€.

Les investissements cumulés de 2012 à 2016 estimés initialement à 21,7 M€ devaient ainsi permettre des gains récurrents annuels de plus de 18 M€ à la cible (2017) et un retour sur investissement inférieur à quatre ans.

Ce modèle budgétaire est confirmé mi-2016 au regard des engagements effectivement réalisés et des migrations des ministères. En effet, alors que les trois quarts du périmètre ont été migrés et mis en facturation sur les marchés du RIE, le coût prévisionnel récurrent annuel en année pleine des réseaux de transport est aujourd'hui actualisé à 53,2 M€.

Ce coût récurrent annuel concerne les réseaux de collecte capillaire ministériels (42,5 M€ essentiellement supportés par les programmes budgétaires des administrations centrales bénéficiaires), le socle interministériel mutualisé[2] (7,1 M€ supportés par le programme 129 « Coordination du travail gouvernemental » sur le BOP SGMAP), ainsi qu'une estimation à 3,5 M€ du restant à la charge des ministères après migration pour leurs infrastructures spécifiques.

[1] *Direction interministérielle du numérique et du système d'information et de communication de l'Etat : article 5 du décret n° 2015-1165 du 21 septembre 2015 relatif au secrétariat général pour la modernisation de l'action publique.*

[2] *L'offre de services mutualisés au sein du socle interministériel est destinée à s'accroître au bénéfice des échanges interministériels. Par exemple, plusieurs des principaux* data centers *interministériels étant colocalisés avec les points d'interconnexion au cœur de réseau RIE, leur raccordement s'effectue directement sur le cœur de réseau mutualisé. De plus, le RIE propose un catalogue de services d'infrastructure en progression (services de nommage d'ores et déjà mis en œuvre, services fédérateur d'annuaire et de routage de messages électroniques pour l'interministériel en projets). Enfin, l'activité de sécurité opérationnelle du RIE contribue à la sécurisation et la défense des systèmes d'information ministériels par une surveillance continue des infrastructures du RIE.*

La maîtrise des coûts d'investissements et de fonctionnement du socle interministériel a permis de financer, au sein de l'enveloppe initialement allouée, le déploiement et l'exploitation des passerelles d'accès sécurisé à internet.

6. Une capacité centralisée de détection des attaques informatiques

L'ANSSI a développé depuis 2010 une capacité centralisée de détection des attaques informatiques visant les systèmes d'information des services de l'État.

Dans ce cadre, elle déploie sur leur réseau des sondes dont elle assure la mise en œuvre et le maintien en condition opérationnelle. Le COSSI est chargé de leur supervision. En 2015, plus d'une dizaine de déploiements ont permis d'améliorer cette activité. La prochaine étape est l'installation, sur le réseau interministériel de l'État (RIE), de sondes de nouvelle génération, capables de supporter de très hauts débits.

L'ANSSI assure également la collecte et la qualification des vulnérabilités et des codes qui les exploitent. En 2015, ses équipes ont identifié plus de 2 300 codes malveillants. Elles ont également rédigé près d'une vingtaine de rapports d'analyse. Elles ont, en outre, publié 568 avis sur des correctifs de sécurité et diffusé 15 alertes sur des vulnérabilités critiques. L'agence est par ailleurs chargée de l'anticipation et de l'analyse des risques et des menaces. En cas d'incident majeur, ses équipes réalisent notamment des notes de synthèse à destination des autorités gouvernementales.

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.

L'agence, via la permanence opérationnelle du COSSI, active 24 heures sur 24 et 7 jours sur 7, reçoit et effectue ensuite un premier traitement des signalements d'événements de sécurité numérique. Le COSSI traite tous types d'événements de sécurité informatique, rapportés par les sondes de détection installées par l'ANSSI, des partenaires français ou étrangers ou encore les victimes. En cas de nécessité, les équipes du centre peuvent se rendre sur place.

En 2015, l'activité de réponse aux incidents a connu une importante croissance : 4 000 signalements ont été reçus, soit 50 % de plus qu'en 2014. Cette augmentation est notamment due au développement, par des prestataires privés, de services de détection des attaques au profit des entreprises. Après investigation, un grand nombre de signalements se sont avérés être des incidents de sécurité et ont été traités par le COSSI. Ce travail a permis de constater l'émergence de nouvelles attaques, dont les « rançongiciels », des logiciels malveillants chiffrant les données d'une ordinatrice victime qui sont alors prises en otage le temps de payer une rançon.

En cas d'attaque de grande ampleur - comme le sabotage ou la prise de contrôle du système d'information à des fins d'espionnage –, une procédure spécifique de gestion est mise en place. En 2015, l'ANSSI a mené une vingtaine d'opérations de cet ordre. L'agence a non seulement travaillé à reprendre le contrôle des systèmes d'information victimes et à remettre en état les éléments compromis, mais aussi à renforcer leur sécurité.

En cas d'événement exceptionnel, l'ANSSI met en place un dispositif de crise, afin de coordonner les différents acteurs et d'apporter une réponse adaptée. Cette organisation permet également à l'agence d'être particulièrement flexible et réactive. En 2015, elle a été activée à quatre reprises. Lors de ces événements, l'ANSSI a été pleinement intégrée au dispositif interministériel de gestion des crises, quand ce dernier a été activé.

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.

Enfin, les équipes réalisent plusieurs dizaines de prestations d'audit au profit de l'administration ainsi que des opérateurs d'importance vitale privés.

E. L'ÉLARGISSEMENT DU PÉRIMÈTRE D'ACTION DE L'ANSSI, AU-DELÀ DES ADMINISTRATIONS

1. Une assistance aux opérateurs d'importance vitale soutenue par un dispositif réglementaire

Pour la réussite de ses missions auprès des opérateurs d'importance vitale, qui appartiennent au secteur privé (environ 130 acteurs), la loi de programmation militaire 2014-2019, par un dispositif réglementaire, a permis d'engager une dynamique qui devrait permettre d'ici quelques années d'atteindre un niveau acceptable de sécurité des systèmes d'information pour ces opérateurs.

Comme l'indiquait le directeur général de l'ANSSI lors de son audition par la commission : « *La loi de programmation militaire 2014-2019 nous donne les moyens d'imposer à ses opérateurs des obligations dans le domaine de la cybersécurité, au-delà du simple conseil. Nous avons été les premiers au monde à faire ce choix, mais beaucoup d'Etats se rallient à cette méthode désormais. Le conseil n'est pas suffisant, si l'on veut pouvoir mobiliser les acteurs avant qu'ils soient attaqués, il faut passer par une politique réglementaire intelligente. C'est ainsi que la loi a été adoptée en décembre 2013, que les décrets d'application ont été*

publiés en mars 2015 et que les arrêtés qui fixent, secteur par secteur, les règles de sécurité imposées aux opérateurs le sont depuis l'été 2016. Ce délai s'explique par notre volonté de coécrire des règles avec les opérateurs, pour mettre en place une réglementation efficace, soutenable financièrement et humainement, et adaptée à chaque secteur. Nous avons voulu coller au mieux à la réalité du terrain, aux contraintes et à la nature des menaces qui sont celles de chaque domaine. »

Dans le 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-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. En 2016, neuf arrêtés sectoriels ont été publiés par les ministères compétents. Ces arrêtés déclinent la nouvelle réglementation par domaine d'activité.

Vos rapporteurs demandent qu'un indicateur de performance puisse mesurer de façon synthétique les progrès réalisés dans la protection des systèmes d'informations des OIV en fonction de cibles à atteindre et que soient publiés, chaque année, des tableaux de bord sur les infractions constatées.

Cet élargissement conduira à renforcer les structures de coordination, de conseil mais également de contrôle et d'assistance opérationnelle[1]. **Il est important pour l'ANSSI de se positionner à la fois sur des dispositifs réglementaires et de contrôle et sur des dispositifs de conseils et d'assistance.**

2. Une sensibilisation et une assistance en direction des autres secteurs d'activités

S'agissant des entreprises qui ne sont pas opérateurs d'importance vitale, des collectivités territoriales et des particuliers, et comme l'ont confirmé les suites cybernétiques des attaques terroristes menées contre la France en janvier 2015, il manque aujourd'hui un dispositif de proximité permettant de porter assistance aux victimes et de rendre visible l'offre existante en matière de suites judiciaires.

Dans le cadre de la stratégie numérique, un travail est engagé aux fins de combler cette lacune, sous le pilotage conjoint de l'ANSSI et du ministère de l'intérieur, en association avec les autres ministères concernés (économie, justice, secrétariat d'État chargé du numérique).

---

[1] *Par ailleurs, un centre d'assistance aux victimes de cyber malveillance, ciblant les entreprises de toutes tailles ainsi que les particuliers, est mis en place à compter de 2016.*

L'ANSSI pilote la mise en place d'une plateforme numérique accessible *via* internet, notamment destinée à mettre en relation les victimes d'actes de cybermalveillance avec des acteurs du secteur privé susceptibles de les accompagner dans le traitement des incidents de sécurité informatique. Le ministère de l'intérieur est étroitement associé à cette démarche qui devrait également permettre de faciliter le dépôt de plainte. Les administrations compétentes du ministère de l'économie et des finances devraient également apporter leurs compétences lors de la mise en place du dispositif.

La forme juridique qui sera retenue pour ce dispositif permettra d'y associer, outre les administrations concernées, les consommateurs, les prestataires de sécurité informatique, les opérateurs de communications électroniques et les éditeurs. Des contenus de sensibilisations aux bonnes pratiques en matière de comportements numériques seront intégrés dans la plate-forme qui sera également un outil d'alerte informatique et un observatoire « en temps réel » de la menace. Le lancement expérimental de la plate-forme devrait avoir lieu en janvier 2017. Sous réserve d'une évaluation positive, la plate-forme devrait être étendue à l'ensemble du territoire métropolitain avant l'été 2017.

Pour les autres victimes que les opérateurs d'importance vitale et pour répondre notamment aux problématiques des PME, très nombreuses et très vulnérables aux actions de cybermalveillance, l'ANSSI conduit une démarche originale qui consiste à incuber un dispositif d'assistance. Ce dispositif est aujourd'hui élaboré au sein de l'ANSSI en collaboration avec le ministère de l'intérieur avec vocation, d'ici deux à trois ans de devenir autonome, en lien avec l'industrie privée qui a tout intérêt à l'élévation du niveau de sécurité globale.

En parallèle, l'ANSSI a développé une politique de sensibilisation et de communication.

Pour l'ANSSI, cela se traduira notamment par la nécessité de disposer de relais dans ces secteurs d'activités jusque-là éloignés des sujets numériques, ainsi qu'en région auprès des services déconcentrés de l'État, des collectivités territoriales et des entreprises. Elle va ainsi déployer un réseau de correspondants dans les régions afin de développer ses actions d'information et de conseil.

3. La mise en place de l'identité numérique

Le règlement européen n° 910/2014 — dit eIDAS— dont le champ d'application est « *l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur* », entré en vigueur le 1er juillet 2016 a une portée éminemment politique. Il concerne la manière dont les États membres appréhendent les questions de l'identité. Ainsi, le règlement instaure la fin du monopole des États membres dans la délivrance de documents d'identités, notamment ceux à valeur probante.

Le règlement introduit trois niveaux de confiance dans les identités électroniques que pourront fournir les usagers pour l'authentification à une téléprocédure (faible, substantiel, élevé). Seule l'identité numérique de niveau élevé a pour objectif non plus une réduction de risque, mais d'empêcher toute usurpation ou altération d'identité (art. 8 du règlement). Le règlement impose aux États membres la reconnaissance mutuelle des identités numériques publiques ou privées notifiées aux niveaux substantiel ou élevé.

Visant exclusivement les conditions dans lesquelles les usagers européens pourront accéder aux téléprocédures administratives mises en place par les États membres, ce règlement deviendra obligatoire dans sa partie identification en septembre 2018. Il aura une incidence sur l'ensemble des modes d'identification aux services publics et privés accessibles *via* les réseaux de communications électroniques.

La stratégie nationale pour la sécurité du numérique prévoit que chaque Français dispose à terme d'une identité numérique de niveau élevé.

Depuis décembre 2015, le ministère de l'intérieur et le secrétariat d'État au numérique pilotent un groupe de travail auquel ont été associées plusieurs administrations, ainsi que le secrétariat général de la modernisation de l'action publique (SGMAP) et l'ANSSI. Plusieurs arbitrages du Premier ministre restent nécessaires pour préciser la stratégie de l'État dans ce domaine et le mode de pilotage de la conception et du déploiement des identités numériques publiques en application du règlement européen n° 910/2014. Une réunion interministérielle doit avoir lieu à l'automne.

F. L'ANSSI, ACTEUR DE LA CONSOLIDATION DE LA FILIÈRE FRANÇAISE DE SÉCURITÉ INFORMATIQUE

La complexité et le volume des opérations de cyberdéfense est en forte croissance en raison du très haut niveau de complexité des attaques menées à l'encontre des systèmes d'information les mieux protégés. Cela exige, en réponse, la mise en œuvre de moyens techniques plus sophistiqués et la mise en place d'une politique industrielle qui assure à notre pays une capacité de défense souveraine.

Dans cette perspective, l'ANSSI mène des actions de politique industrielle, en étroite concertation avec d'autres administrations, notamment la direction générale des entreprises et la direction générale de l'armement. Ces actions poursuivent deux objectifs principaux :

- développer l'offre nationale de produits et de services de sécurité, dont la pérennité est indispensable pour satisfaire les besoins spécifiques de l'État, au premier rang desquels les solutions de très haut niveau de confiance et de sécurité qui assurent la protection des informations classifiées de défense ;

• favoriser le recours à la qualification, et soutenir l'offre qualifiée, y compris sur les marchés d'exportation.

Les actions de l'ANSSI en matière de consolidation de la filière nationale de sécurité informatique se sont principalement inscrites dans le plan d'action « cybersécurité » de la solution « Confiance Numérique » de la nouvelle France Industrielle. Cette initiative a entraîné la mise en place d'un espace d'échange entre pouvoirs publics et acteurs industriels et le lancement d'un nombre significatif d'actions concrètes, qui se déclinent selon plusieurs volets, principalement :

• un volet lié au financement, avec l'orientation des appels à projets du programme d'investissements d'avenir (PIA)[1] : ces dispositifs ont notamment permis une accélération du développement de deux gammes nationales de sondes de détection d'attaques informatiques, étant précisé que l'ANSSI a par ailleurs passé une convention avec BPIFrance pour offrir des facilités de financement à des PME nationales qui souhaiteraient soumettre leurs produits à des certifications de sécurité[2] ;

• un volet de labellisation qui, outre les labels délivrés par l'ANSSI[3], intègre un label « France Cybersecurity » dont la gestion est assurée par la filière industrielle elle-même[4];

• un volet de formation, avec le recensement des besoins qualitatifs et quantitatifs en personnels formés des entreprises nationales du secteur.

L'année 2016 a été marquée par une intensification des travaux visant à développer l'enseignement de la cybersécurité en France. Le projet *CyberEdu*, lancé par l'agence en 2014, promeut cet objectif au sein de l'ensemble des formations supérieures françaises en informatique.

L'agence s'est parallèlement rapprochée d'organismes publics ou privés chargés de la formation en sécurité du numérique afin de favoriser l'émergence d'une offre nationale à la hauteur des enjeux et des besoins[5]. Ces travaux se sont poursuivis avec la mise en place, par l'ANSSI et en collaboration avec des représentants des organismes de formation et de

---

[1] *Deux appels à projet « sécurité numérique » ont été lancés en 2014 et en 2015, sur des thématiques prioritaires identifiées conjointement par les représentants de l'État et de l'industrie. Ils ont permis le financement de 14 projets de recherche et développement.*

[2] *Des travaux ont par ailleurs été lancés et se poursuivent pour développer la connaissance qu'a l'ANSSI des fonds d'investissement privés, et explorer le rôle que l'ANSSI pourrait jouer pour mettre en relation ces acteurs avec des entreprises innovantes dans son domaine de compétence.*

[3] *Voir infra p.50*

[4] *L'ANSSI reste pour sa part associée à la gouvernance. Le label vise à valoriser l'identité de l'offre française en matière de produits et de services de confiance numérique : à ce jour, ce label a été attribué à 70 solutions nationales et il est régulièrement mis en avant, notamment dans des démarches de promotion à l'export.*

[5] *À ce titre, les nombreux échanges avec la commission nationale de la certification professionnelle (CNCP) permettent à l'ANSSI, depuis fin 2015, de parrainer des formations professionnelles de qualité pouvant être inscrites à l'Inventaire de la commission.*

l'industrie, d'un schéma de labellisation de formations supérieures en sécurité numérique[1] ;

- un volet réglementaire, comportant notamment une simplification des modalités de contrôle des exportations de produits de sécurité, conformément aux demandes des acteurs industriels nationaux ;

- un volet lié à l'achat public, visant à favoriser le recours par les administrations aux produits et services de confiance nationaux, dont la qualité aura été établie : cet objectif s'est notamment traduit par l'établissement d'une convention entre l'ANSSI et l'union des groupements d'achats publics (UGAP) pour faciliter l'intégration des offres nationales de confiance dans les catalogues d'achat public et par la publication d'un guide d'achat à destination des administrations. L'ANSSI peut également procéder à l'acquisition de licence globale libératoire de logiciels de chiffrement qualifiés[2];

- un volet d'exportation[3].

Il convient enfin de noter que les structures de gouvernance et de dialogue public-privé mises en place à l'échelon national au titre de ces différentes actions serviront également de fondement à la consolidation des positions nationales dans le cadre du partenariat public-privé sur la cybersécurité établi en juillet 2016 par la Commission européenne.

G. LA POLITIQUE DE LABELLISATION

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 relais dans la mise en œuvre de ses recommandations. A cet effet, elle mène une politique originale de labellisation et de certification.

L'ANSSI délivre plusieurs types de labels, tant sur des produits que sur des prestataires de service dans le domaine des technologies de l'information. Ces labels, qui permettent de mettre en valeur les offres présentant un bon niveau de sécurité et de confiance, sont un outil primordial dans le développement de la sécurité numérique au sein des administrations et des entreprises. Le recours à des produits ou services labellisés est imposé par la voie réglementaire dans certains cas d'usage. Il est par ailleurs largement recommandé par l'ANSSI dans tous les autres cas.

---

[1] *Voir infra p. 52*

[2] *Voir supra p. 36*

[3] *Avec l'établissement de collaborations entre l'ANSSI et Business France, et plusieurs actions ponctuelles de soutien des acteurs nationaux dans les grands salons internationaux, l'extension de ces activités de soutien à l'exportation figure dans la stratégie nationale pour la sécurité numérique*.

La mise en œuvre des différents dispositifs de labellisation représente un engagement significatif pour l'ANSSI, qui y consacre une trentaine d'ETP.

1. La labellisation de produits

La prise de conscience des enjeux liés à la sécurité du numérique conduit les ministères comme les entreprises à exprimer un besoin croissant de sécurité[1] ; pour l'ANSSI, cela se traduit par une augmentation du nombre de produits et services soumis à qualification ou à certification.

Le décret n° 2002-535 du 18 avril 2002 définit le cadre général du schéma national de certification des produits de sécurité. Il permet à l'ANSSI de délivrer, après une évaluation approfondie par un laboratoire privé agréé, des certificats attestant de la conformité d'un produit aux objectifs de sécurité définis par un commanditaire. Ces certificats n'ont pas nécessairement valeur de recommandation d'usage par l'ANSSI ; une part conséquente des certificats délivrés par l'ANSSI répond à des besoins de sécurité exprimés par des tiers, par exemple par le secteur bancaire, qui exige la certification, selon les objectifs de sécurité qu'il a lui-même définis, des moyens de paiement électroniques.

Au titre de ce schéma de certification, l'ANSSI a délivré 96 certificats en 2015 (nombre comparable à 2014, après une croissance significative sur la période 2010-2014), et procédé à la réactualisation de 120 certificats délivrés antérieurement.

L'ANSSI délivre également un autre type de label, dénommé qualification. Celui-ci, qui repose sur une certification assortie de travaux complémentaires, a explicitement valeur de recommandation par l'ANSSI, qui s'assure de la pertinence des objectifs de sécurité et tient à jour un catalogue des produits qualifiés.

La qualification de produits de sécurité s'inscrit désormais dans trois cadres réglementaires distincts : le décret n° 2010-112 du 2 février 2010 relatif aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, le décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale, et le règlement n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, entré en application au 1er juillet 2016.

Tous cadres réglementaires confondus, l'ANSSI a délivré 13 qualifications de produits en 2015, soit un nombre relativement faible dû principalement aux retards enregistrés par plusieurs projets en cours de qualification. Une augmentation significative est d'ores et déjà constatée en 2016 (12 qualifications sur les six premiers mois). L'ANSSI tient par ailleurs à jour un indicateur LOLF « Taux de réalisation du catalogue objectif des produits de sécurité », représentant le taux de couverture par des produits qualifiés de la typologie des produits nécessaires à la satisfaction des besoins de l'administration. Cet indicateur est en progression constante, en dépit de l'augmentation régulière du périmètre à couvrir. Il convient notamment de signaler l'apparition de nouveaux besoins en matière

[1] *Au sein des ministères, cette tendance a pour effet de multiplier les missions de conseil et d'assistance, les audits de sécurité, ainsi que les déploiements de moyens sécurisés (ISIS, TEOREM, Horus, etc.) avec leur soutien. Voir supra p. 36.*

de sondes qualifiées de détection d'attaques informatiques, qui découlent des nouvelles dispositions en matière de cyberdéfense introduites par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019. Les deux premières sondes répondant à ces exigences ont entamé leurs démarches respectives de qualification en juillet 2016, dans le but d'obtenir ces qualifications d'ici la fin de l'année.

Des travaux conséquents ont été engagés en 2016 afin d'améliorer les processus de certification et de qualification, dans un triple objectif de réduction des délais, d'adaptation aux nouvelles contraintes de produits émergents (objets connectés), et d'uniformisation des processus entre les différents cadres réglementaires applicables. Ces travaux devraient notamment donner lieu à la publication, avant la fin de l'année, d'un processus unifié permettant de mutualiser les travaux débouchant sur des qualifications de produits et d'alléger ainsi significativement les charges qui incombent aux fournisseurs.

2. La labellisation des prestataires de services

L'ANSSI délivre des qualifications à des prestataires de services, dans des métiers critiques pour la sécurité numérique. Ces qualifications, qui s'inscrivent dans les trois mêmes cadres réglementaires que précédemment, attestent à la fois de la compétence des prestataires, et de la confiance qui peut leur être accordée pour la protection des informations sensibles que leurs activités les conduisent à manipuler. A la différence des produits, les qualifications de services reposent sur des référentiels distincts, associés à des exigences spécifiques de compétences, pour chaque type de service.

A ce stade, le domaine des prestataires de service dans les métiers de l'audit de sécurité informatique (PASSI – prestataires d'audit en sécurité des systèmes d'information) a atteint son régime de croisière. Instauré en 2013 au titre du décret de 2010, il compte désormais 18 prestataires qualifiés, et 14 en cours de qualification, auxquels se sont ajoutés en juillet 2016 les 10 premiers prestataires qualifiés selon les dispositions du décret de 2015.

Par ailleurs, l'ANSSI conduit actuellement les derniers travaux préparatoires à la mise en place de trois nouveaux domaines de qualification, pour des prestataires respectivement de détection d'incident de sécurité, de réponse à incident, et d'informatique en nuage (*Cloud Computing*). Ces trois domaines font actuellement l'objet de phases expérimentales avec différents prestataires), qui devraient déboucher sur l'instruction des premières qualifications fin 2016 ou début 2017.

Enfin, le règlement du 23 juillet 2014 a introduit un nombre significatif de nouveaux types de services qualifiés, en matière de certification, d'horodatage et de signature électroniques, qui ont nécessité un important travail préparatoire de l'ANSSI en 2015 et 2016, afin de disposer des référentiels applicables à ces différents prestataires avant l'entrée en vigueur du règlement au 1er juillet 2016.

A l'instar de la qualification de produits, des travaux sont en cours afin d'uniformiser autant que possible ces différents domaines de labellisation, et de mutualiser ce qui peut l'être entre les différents cadres réglementaires applicables.

3. La labellisation des filières de formation

L'ANSSI a mis en place un schéma de labellisation de formations supérieures en sécurité numérique, dans le double objectif de valoriser ces formations et de faciliter l'identification, par les employeurs ou les étudiants, des parcours de formation pertinents.

Le label « *SecNumedu* » s'appuie sur un référentiel de labellisation, dont l'élaboration a été pilotée par l'ANSSI avec la contribution d'industriels, d'écoles, du Pôle d'Excellence Cyber (PEC) et du ministère de l'éducation nationale, de l'enseignement supérieur et de la recherche. Il est attribué pour une durée de trois ans renouvelable et permet à la formation qui en bénéficie de figurer au catalogue « *SecNumedu* », de l'ANSSI.

Les premiers dossiers de candidature à cette labellisation seront reçus par l'ANSSI début septembre, dans un objectif de délivrance des premiers labels en janvier 2017.

H. LE RENFORCEMENT DE L'INFLUENCE DE L'ANSSI DANS LE CADRE D'UNE COOPÉRATION INTERNATIONALE

1. Le rôle de l'ANSSI dans la préparation des positions françaises au sein de l'Union européenne

Les institutions européennes s'approprient davantage le cadre normatif de la sécurité du numérique, ce qui doit conduire l'ANSSI à mieux faire partager son expérience afin que les réglementations adoptées soient compatibles avec les choix nationaux.

L'ANSSI a ainsi participé activement à la négociation sur la stratégie européenne de cybersécurité[1], à la finalisation des *EU Standard Operating Procedures*, négociation du mandat de l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), préparation des éléments

[1] *Audition de M. Guillaume Poupard en octobre 2015: « 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 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

relatifs à la cybersécurité des conclusions des Conseil numérique et défense, travaux de seconde évaluation des produits de sécurité protégeant des informations classifiées, etc.).

Elle a porté, comme chef de file, la contribution de la France à l'élaboration de la directive européenne, sur la sécurité des réseaux et des informations (*Network and Information Security – NIS*)[1] adoptée, après près de trois ans de négociations. Le Parlement européen et le Conseil de l'Union européenne (UE) ont adopté le 6 juillet 2016. Les Etats membres auront jusqu'au 9 mai 2018 pour la transposer dans leur droit national.

Cette directive, qui positionne l'Union européenne en pointe en matière de cybersécurité, prévoit le renforcement des capacités nationales et établit un cadre formel de coopération entre Etats membres, auquel l'ANSSI entend prendre une part active. Elle prévoit également le renforcement de la cybersécurité d'opérateurs issus de secteurs clés ainsi que de certaines plateformes numériques.

La transposition de la directive NIS en France, qui sera assurée par l'ANSSI en lien avec l'ensemble des acteurs concernés, pourra bénéficier des travaux réalisés dans le cadre du renforcement de la cybersécurité des opérateurs d'importance dont la compatibilité avec la directive a été assurée.

L'Agence européenne chargée de la sécurité des réseaux et des systèmes d'information (ENISA) avec laquelle l'ANSSI travaille étroitement, sera chargée d'aider les Etats dans la bonne mise en œuvre de la directive.

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.

2. Les autres enjeux dans les enceintes internationales

En dehors de l'Union européenne, l'ANSSI s'implique au sein des instances internationales actives dans le domaine de la cybersécurité : l'OTAN (Organisation du traité de l'Atlantique nord), l'ONU (Organisation des Nations unies) et l'OCDE (Organisation de coopération et de développement économique). Elle participe à l'élaboration des positions françaises et à leur défense, ainsi qu'à des groupes de travail, mais aussi à des exercices internationaux. Ces activités sont menées en liaison étroite avec les administrations concernées. Grâce à ce travail interministériel, la France est l'un des pays les plus présents dans la majorité de ces organisations.

[1] *https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/*

3. Les partenariats bilatéraux

L'ANSSI développe des relations bilatérales et multilatérales avec ses principaux partenaires de confiance, soit plus de trente pays parmi lesquels l'Allemagne, avec laquelle l'agence a renforcé et rendu public son partenariat autour du développement d'une industrie européenne de la sécurité numérique. Ces échanges, plus ou moins développés, sont de natures variées : dialogue stratégique, coopération opérationnelle…

L'agence contribue par ailleurs à la mise en place d'une coordination interministérielle des activités d'assistance capacitaire. Elle soutient également des opérateurs dans la réponse à des appels d'offres internationaux relatifs au développement d'organisations nationales de cybersécurité. Elle participe enfin à l'ouverture du dialogue avec des pays qui hébergent des menaces importantes pour la France.

III. LE CENTRE DE TRANSMISSIONS GOUVERNEMENTAL (CTG)

Pour assurer une partie de ses missions, le secrétaire général de la défense et de la sécurité nationale dispose, pour emploi et sous son autorité, d'une unité militaire interarmées dénommée Centre de transmissions gouvernemental (CTG). Cette entité, d'un effectif de 178 ETP qui sont des personnels militaires, relève du chef d'état-major des armées et les emplois afférents sont inscrits au budget des services du Premier ministre.

Le CTG a pour missions :

- de mettre en œuvre les transmissions sécurisées des plus hautes autorités de l'État ;
- d'exploiter et de soutenir les systèmes d'information de l'état-major particulier (EMP) du Président de la République et du cabinet militaire du Premier ministre ;
- d'administrer les moyens interministériels sécurisés contribuant à la gestion de crise ;
- d'assurer l'interfonctionnement des messageries formelles des différents ministères ;
- de déployer et soutenir les systèmes interministériels sécurisés conçus par l'ANSSI sur un périmètre géographique limité.

Le centre assure quotidiennement l'administration de la passerelle interministérielle des messageries sécurisées SIMS[1], du réseau de télécommunications résilient RCG[2], de la messagerie interministérielle sécurisée ISIS[3] et du système de téléphonie de niveau secret défense

[1] *Système interministériel de messagerie sécurisée.*
[2] *Réseau cœur gouvernemental est un réseau de fibres optiques dont le SGDSN est propriétaire et qui supporte les systèmes d'information contribuant à la gestion de crise.*
[3] *Intranet sécurisé interministériel pour la synergie gouvernementale.*

TEOREM[1], notamment. A ce jour, le CTG administre un parc de 1 560 stations ISIS déployées sur l'ensemble du territoire métropolitain et outre-mer et de 4 651 postes TEOREM répartis dans le monde.

En 2015, le CTG a fourni les moyens SIC des voyages officiels du Président de la République à l'étranger et outre-mer et a également assuré des missions à bord de l'avion à usage gouvernemental (AUG).

Parallèlement, il a conduit, fait homologuer et certifier des projets majeurs concourant à la sécurisation des communications des plus hautes autorités de l'État.

IV. LE GROUPEMENT INTERMINISTÉRIEL DE CONTRÔLE (GIC)

A. L'ÉVOLUTION SENSIBLE DES MISSIONS DU GIC

La loi n° 2015-912 du 24 juillet 2015 relative au renseignement qui, complétée par la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, encadre le recours aux techniques de renseignement et généralise les principes régissant les interceptions de sécurité depuis 1991. Elle modifie sensiblement les missions du GIC auquel elle confie un rôle central dans l'instruction des demandes, la mise en œuvre et le contrôle des techniques de renseignement.

1. Les missions du GIC

Le décret en Conseil d'État n° 2016-67 du 29 janvier 2016[2] et le décret du 9 juin 2016[3] ont précisé les attributions du groupement.

Dans ce cadre, **les missions du GIC ont été définies par le décret en Conseil d'État n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement (article R. 823-1 du code de la sécurité intérieure)** :
- enregistrer les demandes de mise en œuvre des techniques de recueil de renseignement mentionnées à l'article L. 821-2 et aux II et II de l'article L. 854-2 ;
- enregistrer les autorisations de mise en œuvre des techniques de recueil de renseignement mentionnées à l'article L. 821-4 et aux I, II et II de l'article L. 854-2 ;
- recueillir et conserver les informations ou documents mentionnés à l'article L. 851-1 dans les conditions fixées au chapitre Ier du titre V du présent livre ;

[1] *Terminal cryptographique des réseaux étatiques et militaires.*
[2] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031940885&categorieLien=id
[3] https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=9EB2DC96BAFEEF5E47AA6D39C3EB0071.tpdila12v_1?cidTexte=JORFTEXT000032672675&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000032672666

- centraliser l'exécution des interceptions de sécurité autorisées en application du I de l'article L. 852-1 et de l'article L. 854-8 ainsi que les opérations de transcription et d'extraction des communications interceptées ;
- contribuer à la centralisation des renseignements collectés lors de la mise en œuvre de certaines des techniques de recueil de renseignement ;
- concourir à la traçabilité de l'exécution des techniques de recueil de renseignement.

Le GIC, jusqu'alors chargé d'exécuter les interceptions de sécurité et de recueillir les données de connexion, devient désormais le pivot interministériel de gestion de l'ensemble des techniques de renseignement et assure, pour leur mise en œuvre, un rôle de conseiller auprès du Premier ministre.

Il est un correspondant privilégié de l'autorité de contrôle, la CNCTR, qui doit s'appuyer sur sa structure pour accéder aux données et avec laquelle il doit travailler étroitement et en transparence.

Il assure le circuit de validation des demandes, enregistre les avis et les autorisations, garantit l'homogénéité des procédures de suivi, veille à la conformité du recueil et de l'exploitation aux autorisations octroyées.

Le GIC continue d'assurer sa mission « historique » de réalisation des interceptions de sécurité et de recueil des données de connexion au profit des services de renseignement. Il a l'exclusivité de la relation avec les opérateurs de communications électroniques et avec les fournisseurs de services sur internet dans le cadre de la mise en œuvre des techniques de renseignement, pour lesquelles ils sont susceptibles d'être sollicités.

Pour les autres techniques opérées par les services de renseignement, il est chargé de la centralisation des renseignements recueillis au profit de la plupart des services et en coordonne les modalités dans les autres entrepôts autorisés.

Il doit offrir des garanties de sécurité élevées pour le transport, le traitement et la conservation des informations, et rend compte au Premier ministre de la régularité de l'emploi des techniques de renseignement.

Depuis le décret du 9 juin 2016, le Premier ministre a délégué au directeur du GIC la signature des mémoires en défense du Gouvernement face à la juridiction spécialisée du Conseil d'État compétente en matière de techniques de renseignement. À ce titre, le groupement instruit, en interministériel, des requêtes individuelles adressées à la juridiction spécialisée. Il s'est doté en conséquence d'une compétence juridique.

Il élabore les projets d'instructions d'application du cadre légal qui seront soumis avant la fin de l'année 2016 à la signature du Premier ministre.

Il accompagne les services de renseignement et de sécurité pour conseiller et améliorer l'efficacité du travail de leurs exploitants. Il apporte

enfin un soutien technique à leurs actions et opérations, en veillant à minimiser leurs contraintes administratives.

2. Les modalités de leur mise en œuvre

Peu après la publication du décret du 29 janvier 2016, des arbitrages interministériels ont confié au GIC des missions nouvelles de mise en œuvre de la loi sur le renseignement :

- création d'une direction de programme interministérielle des systèmes d'information concourant à la mise en œuvre du cadre légal des techniques de renseignement, installée au GIC sous la direction du directeur du groupement. Cette direction, constituée d'une équipe réunissant différentes spécialités pour coordonner les choix techniques et les déploiements des systèmes d'information concourant aux techniques de renseignement, soumettra au cabinet du Premier ministre des propositions d'arbitrages stratégiques ;

- centralisation du renseignement. Le GIC proposera au Premier ministre, au terme d'une réflexion qui prendra en compte les impératifs opérationnels et la nécessité du contrôle, un système permettant de centraliser les renseignements recueillis et les résultats de leur exploitation. Afin de faciliter l'accès des services du second cercle aux techniques de renseignement, la répartition sur le territoire des centres d'exploitation du GIC pourra être densifiée. A cet effet, le groupement conduira une étude avec le ministère de l'intérieur pour examiner la création éventuelle de nouveaux centres ;

- en matière de surveillance internationale, la loi dispose que le Premier ministre organise les dispositifs de traçabilité (L. 854-4 du code de la sécurité intérieure). Le GIC participera au développement des outils et effectuera un contrôle permanent de la mise en œuvre et de l'exploitation dans ce domaine ;

- communication des transcriptions des interceptions de sécurité aux services bénéficiaires. Il a été admis que la majorité des transcriptions pouvait être classifiée, non pas au niveau « secret défense » mais au niveau « confidentiel défense ». Dès lors, il devient possible de les transmettre sous forme numérique aux services bénéficiaires dotés de systèmes d'information aptes à assurer leur traçabilité. Le GIC développera en commun avec un service de renseignement, d'abord à titre expérimental, un mécanisme et des procédures de communication dématérialisée des transcriptions d'interceptions de sécurité ;

- création au GIC d'une fonction d'audit de la mise en œuvre des techniques de renseignement par les services. Il effectuera, avec les inspections ministérielles et l'inspection des services de renseignement, des audits de l'emploi des techniques de renseignement par les services et

rendra compte au Premier ministre de la bonne application du cadre légal des techniques de renseignement.

B. LE NÉCESSAIRE CHANGEMENT DE SON FORMAT ET DE SON ORGANISATION

Ces missions nouvelles s'accompagnent d'un changement du format et de l'organisation du groupement, lui permettant de prendre en compte un 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).

1. L'évolution de l'organisation du GIC

Dès la fin du premier semestre 2015, le GIC a commencé à adapter ses structures et son organisation pour prendre en compte les dispositions de la loi relative au renseignement.

Le jour de l'entrée en vigueur du nouveau cadre légal, le GIC s'était doté d'une organisation provisoire pour assurer le circuit de validation des demandes de techniques de renseignement.

Afin de fluidifier le circuit administratif des demandes de techniques de renseignement et de raccourcir les délais de traitement, le développement d'un système automatisé de gestion a été lancé pour être déployé en 2017. Ce système allègera l'augmentation considérable de la charge de travail liée au traitement non automatisé des demandes et permettra à terme l'édition de statistiques ;

Pour la collecte et la centralisation des renseignements, le développement d'applications informatiques *ad hoc* a été initié en relation avec les services de sécurité et de renseignement, selon des modalités propres à chaque technique. La réalisation de ces applications est donc progressive. Leur déploiement sera échelonné au cours des années 2016 et 2017 et permettra une véritable montée en puissance du dispositif technique de contrôle.

S'agissant de son activité historique relative aux interceptions de sécurité, le GIC définit et enrichit son système de recueil et d'exploitation des correspondances.

Enfin, le GIC contribue à la formation et à l'information des agents des services qui recourent aux techniques de renseignement.

2. L'intensification de son activité

L'augmentation et la diversification des techniques autorisées par la loi de 2015, leur extension aux services du second cercle et le contexte

général d'intensification de la lutte contre le terrorisme, se traduisent par une augmentation sensible de l'activité du GIC.

Le nombre de demandes de techniques de renseignement est en constante augmentation, avec une croissance estimée de 50 % entre le dernier trimestre 2015 et le premier trimestre 2016 et de 200 % entre les deux premiers trimestres de 2016[1].

Vos rapporteurs estiment souhaitable qu'au fur et à mesure du déploiement de ses nouvelles missions, le GIC puisse produire une batterie d'indicateurs pour mesurer le niveau de son activité.

3. Une situation administrative en cours de stabilisation

En termes de fonctionnement, la situation administrative du GIC est en cours de stabilisation.

Les textes réglementaires nécessaires à la définition précise de son statut de service administratif seront pris en 2016, afin d'en faire un service à compétence nationale, comme le recommandait dans son rapport pour 2015 la délégation parlementaire au renseignement.

La révision du statut de l'ensemble de ses personnels[2] a été initiée en 2016.

Le GIC bénéficiera du soutien administratif et financier du SGDSN, notamment dans le cadre des procédures adjudicatrices et dans la programmation et la gestion du budget en fonds normaux[3], tout en relevant directement du Premier ministre pour son activité opérationnelle.

---

[1] *Estimation qui devra être confirmée par la CNCTR dans son rapport annuel dont la publication est attendue pour la fin du mois de novembre 2016.*

[2] *Voir infra p.69*

[3] *Voir infra p.78*

TITRE 2 : LES MOYENS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2017

Le budget opérationnel de programme (BOP) du SGDSN dans le projet de loi de finances pour 2017 s'élève à **282 millions d'euros** en autorisations d'engagements **(**267,8 en 2015) et **277,5 millions d'euros** en crédits de paiement 255,81 en 2016) **et un plafond de 895 ETPT.**

CRÉDITS DU BOP SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2017

(EN MILLIONS D'€)

	Exécution 2015		**LFI 2016**		**PLF 2017**	
	AE	CP	AE	CP	AE	CP
Titre 2	*62*	*62*	*70,7**	*70,7**	*84,4*	*84,4*
HT2	*129,8*	*157,9*	*197,1**	*185,1**	*197,7*	*193,1*
TOTAL	**191,8**	**219,9**	**267,8**	**255,8**	**282,1**	**277,5**

**en tenant compte de l'adossement du GIC en gestion (11,5 M€ hors T2 et 3,9 M€ en T2)*

Son évolution 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 plus de la moitié des effectifs budgétaires (545 ETPT), des efforts d'investissement et des crédits de fonctionnement du SGDSN. 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).

Jusqu'en 2015, le budget du GIC était retracé au sein du BOP « Soutien » du programme 129 (centre financier « Autres dépenses ») et son financement était constitué essentiellement de fonds spéciaux. Depuis le 1er mai 2016, le soutien administratif et financier du GIC est assuré par le SGDSN.

Depuis le 1er mai 2016, la moitié des agents du GIC est sous contrat du SGDSN et la part de son budget, constituée de crédits de droits commun, est gérée par le SGDSN qui assure son soutien administratif et financier. Les

crédits et les emplois de ce service ont vocation à faire l'objet d'un adossement en gestion sur le budget opérationnel de programme. Dont il est devenu une unité opérationnelle

I. LES CRÉDITS DE TITRE 2 ET LA POLITIQUE DES RESSOURCES HUMAINES

A. LES CRÉDITS ET LES EMPLOIS INSCRITS AU BOP SGDSN

EFFECTIFS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2017

	LFI 2016*		**PLF 2017****	
	ETP	ETPT	ETP	ETPT
ANSSI	497*	507	547	545
CTG	178	178	178	178
SGDSN hors ANSSI et CTG	209	210	212	216
Total SGDSN	**884**	**895**	**937**	**939**
GIC	85	80	189	174
BOP SGDSN	**966**	**975**	**1 126**	**1 113**

**en tenant compte de l'adossement du GIC en gestion (11,5 M € hors T2 et 3,9 M € en T2)*

1. L'évolution des emplois et des crédits de personnel de 2010 à 2016.

Sur la période 2010-2016, l'évolution des crédits du SGDSN est principalement marquée par l'augmentation des effectifs de l'ANSSI, qui atteignent 460 ETP à la fin de l'année 2015. Le schéma d'emplois de cette agence est de 40 ETP en 2016[1].

Hors ANSSI, le plafond d'emplois du SGDSN pour les secteurs non prioritaires a subi une diminution globale de 25 emplois sur la période 2010-2016, avec une décélération de cette tendance les trois dernières années (-1 ETP chaque année).

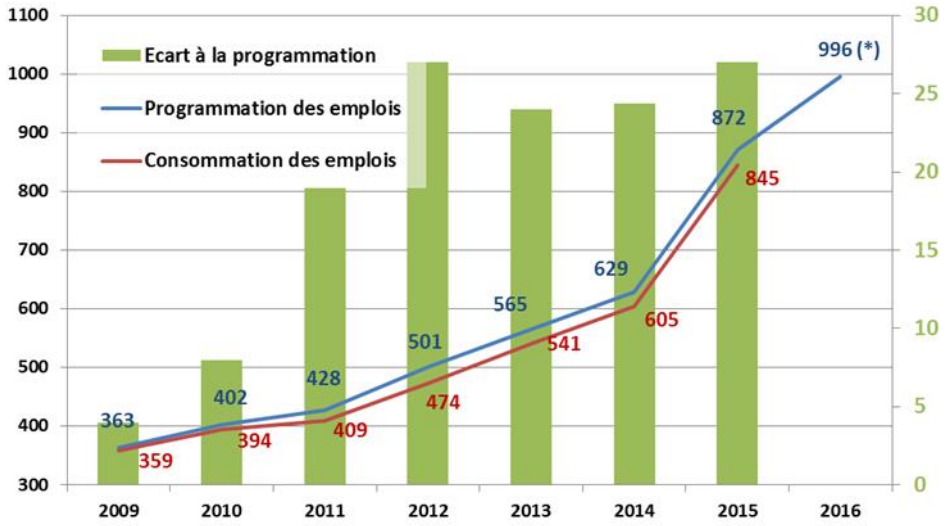
Par ailleurs, en application du décret du 12 juin 2014, les effectifs du centre de transmissions gouvernemental (CTG), unité militaire mise pour emploi auprès du secrétaire général de la défense et de la sécurité nationale,

[1] *Mesure corrigée en gestion à +37 ETP pour permettre le gage de 3 emplois de soutien liés à l'adossement du GIC. Ces 3 emplois ainsi gagés sont restitués à l'ANSSI au travers de son schéma d'emplois pour 2017.*

s'ajoutent au plafond d'emplois du BOP SGDSN à compter de 2015 (179 ETP).

En 2016, les effectifs du groupement interministériel de contrôle (GIC) ont également été ajoutés au plafond d'emplois du SGDSN, pour un total de 60 ETP en socle (mesure de périmètre en LFI 2016), auxquels s'ajoutent 25 ETP sur le schéma d'emplois (20 ETPT).

Le graphe ci-après synthétise l'évolution des emplois en programmation et en exécution, à périmètre constant, sur la période 2015-2016 (en ETP).

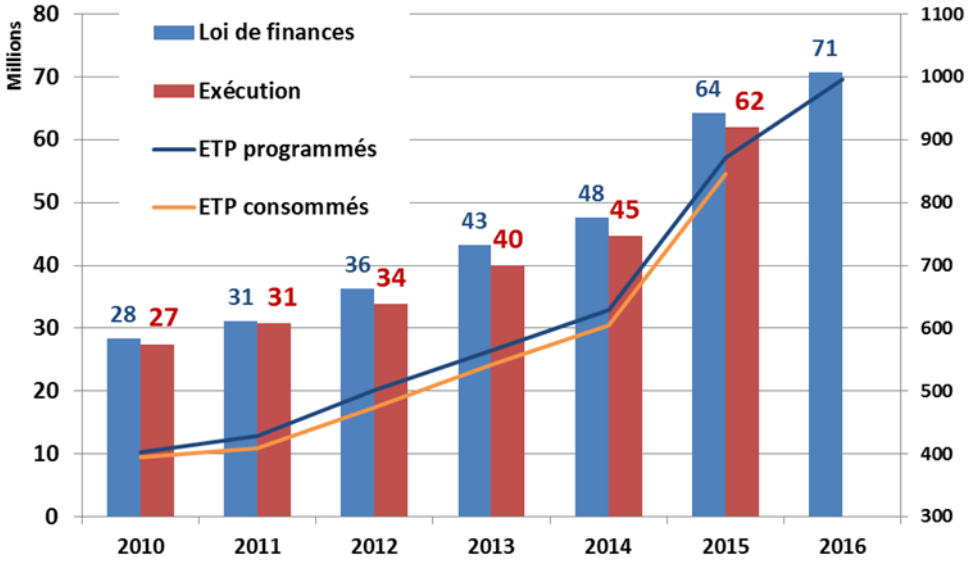


(*) Cible de la LPFP 2015-2017 en ETP

Source : SGDSN réponse au questionnaire parlementaire

L'évolution des crédits du titre 2 suit celle des effectifs et des changements de périmètre (CTG, GIC) intervenus. Ainsi, en 2016, 66,8 M€ de crédits ont été votés pour le SGDSN mais l'adossement du GIC en gestion, à compter du 1er mai 2016, a conduit à une majoration des crédits ouverts à 70,7 M€.

Le graphique suivant met en perspective l'évolution des crédits de masse salariale (programmation et exécution sur l'ordonnée de gauche) avec celle des emplois (ordonnée de droite).



Source : SGDSN réponse au questionnaire parlementaire

2. L'évolution des emplois et des crédits de personnel demandés en PLF 2017

LFI 2016	PLF2017			
	Mesures nouvelles	Total à périmètre constant	Mesures de transfert	Total à périmètre courant
AE/CP	AE/CP	AE/CP	AE/CP	AE/CP
70 730 695	8 452 016	79 191 710	5 275 348	84 467 059

En 2017, l'évolution de la dépense du titre 2 s'explique en premier lieu par les évolutions suivantes du schéma d'emplois :

- ANSSI : 50 ETP (25 ETPT), permettant à l'agence d'atteindre 547 ETP fin 2017 ;
- GIC : 35 ETP (20 ETPT), permettant à ce service d'atteindre 120 ETP fin 2017, hors mesures de transfert ;
- Administration générale : 3 ETP pour assurer le soutien administratif et financier du GIC.

En outre, les mesures de transfert entrant suivantes sont également prévues, qui portent *in fine* les effectifs du GIC consolidés sur l'ensemble de son nouveau périmètre à 189 ETP[1] :

- 60 ETPT du ministère de la défense, correspondant à des emplois d'ores et déjà en place au sein du GIC ;
- 9 ETPT du ministère de l'intérieur, destinés à mettre en place un dispositif de sécurité armé par des gendarmes sur une seconde emprise parisienne du GIC.

B. LE SGDSN : UN INTÉGRATEUR QUI DOIT SE DOTER DES MOYENS EN PERSONNELS EN MESURE DE SOUTENIR UN ENSEMBLE HÉTÉROGÈNE DE STRUCTURES

Le SGDSN a connu une évolution considérable au cours des dernières années. Il est devenu la structure de portage d'un ensemble d'entités plus ou moins autonomes qui aujourd'hui, tant en crédits qu'en effectifs, dépasse largement le »cœur historique » du secrétariat général.

Si l'ANSSI et le GIC ont vu leurs moyens croître pour faire face à des missions élargies, ce n'est pas le cas des directions et service du SGDSN. Or le contexte de sécurité nationale fait peser une charge accrue sur un nombre peu élevé d'agents.

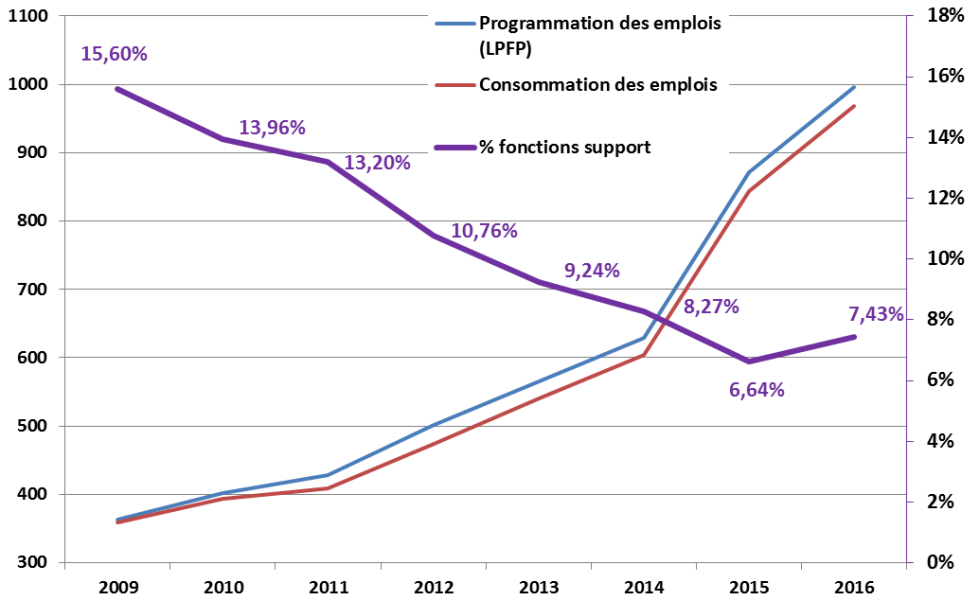
Le SGDSN a en effet été largement mis à contribution lors de la révision générale des politiques publiques entre 2008 et 2009 :

- deux directions centrales ont été supprimées, soit par fusion, la direction des technologies des transferts sensibles et des affaires internationales stratégiques ayant fusionné en une direction unique des affaires internationales, stratégiques et technologiques (AIST), soit par requalification en service de la direction de l'administration générale ;
- les emplois de coordination ont été réduits d'un quart (- 10 emplois sur 40) ;
- deux entités ont été transférées (le comité interministériel du renseignement et le haut responsable de l'intelligence économique), bien que certaines de leurs attributions aient été maintenues au sein du SGDSN (secrétariat du CNR par exemple).

Si on exclut l'ANSSI du périmètre considéré (388 créations d'emplois en 2008-2016), 21 emplois ont été supprimés et 24 transférés. Hors ANSSI, la réduction de 21 emplois représente plus de 9 % des effectifs de 2008.

---

[1] *Le GIC comprend en outre 15 ETP relevant de la gestion du ministère de la défense, qui ont vocation à être transférés vers le SGDSN avant le 1er janvier 2018. En prenant en compte les personnels mis à disposition du GIC par le ministère de la défense au 1er janvier 2017 (15 ETP), les effectifs du groupement sont* in concreto *de 195 ETP, auxquels s'ajoutent les 9 ETP pour la sécurité du second site parisien.*



Source : SGDSN

L'une des conséquences de ces mesures de suppression est l'impact sur le soutien dont les effectifs représentaient en 2009, 15,6 % du total. Ce *ratio* était conforme à celui de l'ensemble des services du Premier ministre. Avec une réduction des effectifs de soutien et un accroissement des effectifs à soutenir au sein de l'ANSSI, la proportion de personnel affecté à des tâches de soutien est tombée en 2013 à 9,24 %. En 2016, ce *ratio* qui affichait en début d'année 6,6 % est remonté à 7,43 %, après redéploiement d'effectifs sous plafond pour permettre l'adossement du GIC au SGDSN dans de meilleures conditions.

Il ressort de cette analyse que le SGDSN est sans doute parvenu à l'étiage en 2015, point au-dessous duquel la poursuite des mutations en cours serait difficile. Il devra, en conséquence, veiller à renforcer cette fonction pour assurer efficacement le pilotage et la coordination de cet ensemble et notamment l'adossement administratif du GIC.

S'il est entendu que la vocation du SGDSN est de demeurer une administration de mission d'une taille maitrisée, cette caractéristique ne doit pas devenir une faiblesse, alors que les missions qui lui sont confiées se développaient en intensité et en diversité.

Vos rapporteurs estiment que cette situation doit faire l'objet d'une attention vigilante.

C. L'ANSSI : POURSUIVRE LA MONTÉE EN PUISSANCE EN CONSERVANT LE NIVEAU DE COMPÉTENCE ET D'EXPERTISE

L'effort en faveur de la croissance des effectifs de l'agence depuis sa création doit être poursuivi en 2017. En effet, l'agence doit non seulement assurer ses missions habituelles dont la charge est en croissance permanente,

notamment en matière de traitement des attaques informatiques, mais elle doit également répondre à l'évolution de la menace, à la mise en œuvre de la loi de programmation militaire (LPM) et de la directive européenne NIS sur la sécurité des réseaux des opérateurs essentiels. Elle doit également contribuer aux réponses à apporter aux besoins croissants de sécurisation des entreprises et des particuliers. Les éléments de cette réponse sont donc fonction de l'évolution de la charge de travail, des usages et de la menace tels qu'ils sont prévisibles.

La croissance des effectifs a d'ores et déjà permis à l'agence de passer de 122 ETP en 2009 à 460 ETP fin 2015. Les évolutions opérationnelles prévisibles à l'horizon de deux ans conduisent à autoriser le recrutement de 50 ETP sur le schéma d'emplois en 2017. A la fin de l'année prochaine, l'agence devrait ainsi compter à 547 ETP. L'ANSSI considère toutefois que son effectif devrait être d'une centaine d'agents supplémentaires pour être en mesure de réaliser l'ensemble de ses missions.

Sous-directions	**Effectifs fin 2016**	**Effectifs fin 2017**
Centre opérationnel de la SSI (COSSI)	168	185
Sous-direction expertise (SDE)	145	159
Systèmes d'information sécurisés (SIS)	87	97
Relations extérieures et coordination (RELEC)	61	68
Sous-direction affaires générales (SDAG)	18	20
Autres	18	18
Effectif total ANSSI	**497**	**547**

Source : SGDSN – réponse au questionnaire parlementaire

En 2015, 108 salariés ont rejoint l'ANSSI, dont 15 en fin d'études. Les deux tiers du personnel faisaient partie du Centre opérationnel de la sécurité des systèmes d'information (COSSI) et de la sous-direction Expertise (SDE). Du fait du domaine d'activité de l'agence, en constante évolution, 25 % des agents étaient âgés de moins de 30 ans, et 40 % avaient entre 30 et 40 ans. Enfin, trois quarts des agents étaient des contractuels, dont 73 % en CDD et 27 % en CDI. Le reste du personnel est composé de militaires (11 %) et de fonctionnaires (14 %). En effet, les profils recherchés par l'ANSSI sont rares dans la fonction publique.

Dans le cadre de sa stratégie à l'horizon 2020, l'ANSSI a souhaité améliorer son fonctionnement général en assurant notamment une meilleure gestion des fonctions relatives aux ressources humaines. Pour y parvenir, elle a adopté une politique de ressources humaines à la fin du premier semestre 2016. Celle-ci doit non seulement permettre à l'agence de réaliser ses recrutements, de répondre aux attentes de son personnel, mais aussi de

donner des orientations précises sur les objectifs à atteindre aux agents chargés de cette gestion. Ces objectifs peuvent ainsi être synthétisés en trois volets complémentaires :

- une gestion renforcée des ressources humaines où chaque processus est révisé afin d'être optimisé ;

- une meilleure information et visibilité au bénéfice des agents : chacun d'entre eux doit être en mesure de connaître les conditions de son emploi et d'envisager un parcours professionnel cohérent ;

- une meilleure attractivité et fidélisation des agents : les actions à mener visent au recrutement d'agents dont les compétences et les qualités répondent aux besoins pour une durée suffisamment longue.

La montée en puissance reste un défi structurel de l'agence qui doit également pourvoir au *turn over* relativement important de ses agents dont nombre sont, compte tenu de leur spécialité, des contractuels. Elle doit à la fois recruter en nombre et maintenir la qualité de ce recrutement.

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 permet également l'émergence d'un réseau lorsque les industriels qui embauchent ces personnels sont considérés comme de confiance. Ceci constitue un aspect positif pour la diffusion d'un « culture » de la cybersécurité.

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 demeure 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 recherchent des profils analogues ou voisins, sans parler des entreprises du secteur privé et des administrations publiques, de plus en plus sensibilisées à la cybersécurité, et qui souhaitent renforcer leurs direction des systèmes d'information, ou enfin, d'entreprises de prestations de services spécialisées dans ce domaine. Vos rapporteurs approuvent l'engagement de l'ANSSI dans une politique de labellisation des formations universitaires, mais cet effort

doit être conforté par une action plus intense du ministère de l'enseignement supérieur et de la recherche pour orienter les universités et les grandes écoles à développer ces filières d'avenir. La formation est aussi un investissement d'avenir.

D. LE GIC : GARDER LA MAÎTRISE DE SES EFFECTIFS ET ASSURER LEUR MONTÉE EN PUISSANCE

1. Le transfert au GIC de la gestion administrative de son personnel et son adossement au BOP SGDSN

Les dépenses de personnel ne couvrent, jusqu'en 2015, que la rémunération des agents employés en vertu d'un contrat GIC et la prime spécifique du GIC versée à l'ensemble des agents. Elles sont relativement stables. Elles prennent en compte les effets des travaux de refonte des grilles indiciaires et du régime indemnitaire spécifique des personnels du GIC.

Une décision du Premier ministre en date du 25 février 2003 a fixé à 90 le nombre de postes mis à disposition du GIC par le ministère de la défense[1], cet effectif pouvant être complété par le recrutement de 60 agents sur des contrats rémunérés par les services du Premier ministre. En 2015, le GIC a amorcé une montée en puissance dans la perspective de la mise en œuvre de la loi relative au renseignement. La gestion administrative des personnels du GIC était alors assurée par le ministère de la défense.

Alors que l'ensemble des personnels du GIC était auparavant géré par le ministère de la défense, à la suite de l'évolution des missions du GIC, et comme l'a recommandé la délégation parlementaire au renseignement[2], les personnels du GIC sont en cours de rattachement au BOP SGDSN.

Une fraction des personnels est, depuis le 1er mai 2016, placée sous contrat des services du Premier ministre (SGDSN). L'adossement du GIC au SGDSN s'est traduit, en gestion 2016, par le rattachement au BOP des emplois ayant fait l'objet d'une mesure de périmètre en LFI 2016 (60 ETP) auxquels s'ajoutent les nouveaux effectifs correspondant au schéma d'emplois (25 ETP pour 20 ETPT). A fin juin 2016, 71,9 ETP sur les 85 ouverts sont affectés au GIC, ce qui permet de conjecturer une consommation des emplois à hauteur du volume disponible[3].

En 2017, l'évolution des effectifs du GIC s'explique par :

- un schéma d'emplois de 35 ETP (20 ETPT) ;

---

[1] En 2014, 12 postes ont été transférés à la DGSE, qui a pris à son compte l'effectif de la section d'exploitation en charge du traitement de ses interceptions de sécurité.

[2] Rapport 2015 de la DPR p. 36.

[3] Exception faite du directeur du GIC, d'un cadre A de la fonction publique et de deux catégories B, les emplois actuellement gérés par le SGDSN sont des emplois contractuels.

• un transfert entrant de 9 ETPT dont 4 depuis le programme 152 « Gendarmerie nationale » et 5 depuis le programme 176 « Police nationale » de la mission « Sécurité » et 0,73 million d'euros, transférés au titre du renforcement du dispositif de sécurité des emprises du GIC. Ces personnels doivent assurer la sécurité d'une nouveau centre d'exploitation du GIC ouvert mi-2016.

• un transfert partiel au GIC des personnels de la DGSE déjà affectés au GIC. Il s'agit de 75 postes. Un droit d'option a été ouvert aux personnels concernés, jusqu'au 30 septembre 2016. Avant de connaître les souhaits des intéressés, il a été arrêté que seuls 60 postes[1] seraient transférés[2] au 1er janvier 2017 puisque le reliquat de 15 postes serait transféré au plus tard le 1er janvier 2018. Les personnels ont depuis exercé leur droit d'option pour continuer leur carrière professionnelle au sein du groupement.

Cette évolution est indispensable pour garantir au GIC son autonomie. Vos rapporteurs s'interrogent sur le fractionnement des transferts en provenance du ministère de la défense, d'autant que le GIC a des besoins à pourvoir immédiatement et ne peut se passer de ces personnels qui, en outre, ont opté pour rester. Ils souhaiteraient que cette évolution soit complètement achevée au 1er janvier 2017, conformément à la première proposition du rapport de la délégation parlementaire au renseignement.

Les effectifs du GIC, sur le périmètre du SGDSN, devraient donc évoluer de 85 ETP en 2016 à 189 ETP en 2017. La masse salariale correspondante devrait ainsi passer de 4,1 M€ en LFI 2016 à 10,9 M€ en PLF 2017. Ce montant correspond pour 7,4 millions d'euros à des rémunérations d'activité, pour 3,3 à des cotisations et contributions sociales (y compris les cotisations aux CAS Pensions) et pour 0,17 million à des prestations sociales et allocations diverses.

2. La politique des ressources humaines du GIC

La politique du GIC en matière de ressources humaines obéit à deux impératifs :

• l'un quantitatif, pour répondre à l'évolution des missions du GIC, mais aussi à l'augmentation sensible des demandes de mise en œuvre de techniques de renseignement qui résulte tout à la fois de la mise en œuvre de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, complétée par la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de

[1] *et de 4,55 millions d'euros depuis le programme 212 « soutien de la politique de la défense » de la mission « défense ».*

[2] *Ce transfert concerne 39 militaires (5 officiers, 34 sous-officiers) et 21 fonctionnaires (3 catégorie A, 9 catégorie B et 9 catégorie C. A la différence des fonctionnaires qui seront payés directement par le SGDSN, la prise en charge des militaires s'effectuera par le biais de rétablissements de crédits (hors PSOP).*

surveillance des communications électroniques internationales et du contexte général d'augmentation des menaces et de l'utilisation des techniques dans le cadre de la lutte contre le terrorisme ;

• L'autre qualitatif, par une requalification des catégories d'emplois : majoritairement armé par des personnels de catégories B et C, le GIC était historiquement un service opérationnel d'exécution, appliquant des procédures établies ; il doit à présent, au regard de la multiplication des systèmes informatiques et de ses nouvelles missions, recruter des personnels hautement qualifiés et des développeurs[1].

Pour mener ses nouvelles missions d'audit des services dans le cadre de la centralisation du renseignement, réalisé par la mise en œuvre de techniques de recueil de proximité, le GIC doit ainsi développer de nouvelles compétences, constituer des équipes et élaborer des procédures inédites. En outre, la délégation donnée au directeur du GIC par le décret du 9 juin 2016 pour représenter le Premier ministre face à la juridiction spécialisée du Conseil d'État a nécessité de créer au GIC une compétence juridique de haut niveau afin d'analyser la régularité de certaines demandes de mise en œuvre de techniques de renseignement, de traiter avec la CNCTR les points d'attention et d'instruire des requêtes individuelles, voire des recours, devant la juridiction spécialisée.

Une revue générale des processus RH, des statuts des personnels et des régimes indemnitaires a été engagée afin de se conformer aux dispositions en vigueur dans les services du Premier ministre.

En mai 2015, le GIC avait conduit une première étude montrant le besoin d'une augmentation progressive de ses effectifs, avec une cible de 200 ETP en 2020. Cette projection résultait à la fois de la mise à niveau des effectifs du groupement devenus insuffisants pour assurer ses missions historiques[2], mais aussi d'une estimation des besoins relatifs aux nouvelles missions qui seraient confiées par la loi sur le renseignement. Après adoption de la loi, plusieurs arbitrages ont conduit à revoir la cible, ainsi que le rythme de progression des recrutements. Cette révision s'est aussi appuyée sur les recommandations de l'inspection des services de renseignement, qui ont reçu un arbitrage favorable du Premier ministre.

Au total, le besoin en effectifs du GIC a été augmenté de 20 ETP à l'horizon 2020 selon la chronique suivante :

[1] *L'augmentation de la proportion de cadres de niveau A aura une conséquence sur la rémunération moyenne des agents du GIC, intégrée dans la valorisation de la masse salariale pour 2017.*

[2] *Mise en œuvre des interceptions de sécurité et au recueil des informations auprès des opérateurs.*

	2015	2016	2017	2018	2019	2020
En ETP	132 (*)	160	195 (**)	206	213	220

(*) Effectifs réalisés au 31 décembre 2015.

(**) Hors prise en compte des gendarmes chargés de la sécurité sur la nouvelle emprise immobilière (9 ETP). En revanche, est pris en compte le volume des agents du ministère de la défense restant à transférer (15 ETP).

L'intensification de la lutte contre le terrorisme et l'extension, par le décret du 11 décembre 2015, des services autorisés à utiliser les techniques de renseignement visées par la loi, sont susceptibles d'accroître le niveau d'activité du GIC. Vos Rapporteurs souhaitent que le Premier ministre se montre particulièrement vigilant pour sécuriser la montée en puissance du GIC qui constitue le point sensible de la mise en œuvre efficace de la loi relative au renseignement : un engorgement dans l'instruction des demandes de techniques de renseignement, ou des insuffisances dans le recueil et la conservations des données, voire une incapacité pour la CNCTR d'effectuer les contrôles nécessaires, seraient particulièrement dommageables.

En outre, un enjeu important pour la direction du GIC sera de réussir à maintenir la cohésion au sein d'un service caractérisé par la mixité de son personnel, issu d'administrations différentes, avec des statuts, des modes de gestion et de rémunération différents et qui, en outre, va être amené à recruter dans les prochaines années un grand nombre de collaborateurs (création de postes et *turn over*). Pour vos Rapporteurs, il s'agit là d'un processus de transformation important qui devra être suivi et piloté attentivement.

II. LES CRÉDITS DE FONCTIONNEMENT ET D'INVESTISSEMENT INSCRITS AU « BOP » SGDSN

L'évolution des crédits et des emplois est sensiblement affectée par l'adossement administratif et financier du groupement interministériel de contrôle (GIC) depuis le 1er mai 2016 qui modifie le périmètre du budget opérationnel de programme (BOP) « SGDSN », sans pour autant modifier l'architecture du domaine fonctionnel du programme 129.

En 2017, les crédits du GIC restent en effet retracés dans une sous-action spécifique de l'action 2 « Coordination de la sécurité et de la défense », distincte de celle où sont hébergés les crédits du SGDSN à périmètre constant.

Crédits hors titre 2 avec GIC :

	LFI 2016		PLF 2017	
	AE	CP	AE	CP
SGDSN "programmes transverses"	12 451 179	**12 715 318**	10 510 382	**11 032 991**
SGDSN - CTIM	82 689 688	**76 156 655**	82 312 291	**82 749 228**
SGDSN - ANSSI	73 660 293	**67 902 736**	72 427 041	**66 871 000**
SGDSN - opérateurs	16 817 500	**16 817 500**	15 819 824	**15 819 824**
SGDSN - GIC (hors fonds spéciaux)	13 994 136	**13 994 136**	16 607 802	**16 607 802**
TOTAL	199 612 796	**187 586 345**	197 677 341	**193 080 845**

Source : SGDSN – réponse au questionnaire parlementaire

A. SGDSN/ANSSI : DES ACTIONS NOMBREUSES ET DIVERSES À SOUTENIR

1. Les crédits hors titre 2 en 2016

En 2016, 185,6 M€ d'AE et 173,6 M€ de CP ont été ouverts en loi de finances pour le BOP SGDSN sur les crédits hors titre 2. Le montant total de la mise en réserve initiale s'établit à 14,1 M€ en AE et 13,1 M€ de CP. L'adossement du GIC en gestion, a entraîné une majoration de 14 M€ d'AE et de CP sur le périmètre du SGDSN[1] . En outre, une mesure d'annulation en AE=CP de 5,8 M€, dont 1,8 M€ sur le GIC et surgel de 0,5 M€ en AE=CP est intervenue dans le cadre d'une taxation interministérielle destinée au financement de plusieurs mesures gouvernementales, au travers du décret d'avance du 2 juin 2016[2].

S'agissant des mouvements réglementaires de crédits, le SGDSN prévoit le transfert de 95,8 M€ d'AE et de 88,4 M€ de CP en 2016 par deux décrets publiés respectivement le 21 octobre et le 4 novembre.

Comme les années précédentes, les transferts de crédits vers les programmes 144 « Environnement et prospective de la politique de la défense », 146 « Équipement des forces » du ministère de la défense et 176 « Police nationale » s'inscrivent dans le cadre de la mission de pilotage et de coordination confiée par le Premier ministre au secrétaire général pour ce qui concerne les investissements relatifs à la sécurité nationale[3], notamment dans le domaine de la sécurité des systèmes d'information. Il est ainsi prévu de contribuer principalement aux financements :

[1] *En LFI 2016, le GIC bénéficiait d'une ouverture de 14 M€ de crédits de droit commun en AE=CP (hors fonds spéciaux), donnant lieu à un disponible de 12,9 M€. 1,3 M€ d'AE et de CP ont par ailleurs été consommés avant l'adossement au SGDSN intervenu le 1er mai 2016.*

[2] *Décret n° 2016-732 du 2 juin 2016.*

[3] *A ce titre, il est chargé de la cohérence de ces investissements à caractère confidentiel et dispose de crédits budgétaires dont il assure la répartition en cours de gestion, en fonction de l'avancement des programmes des différents services de l'État.*

- d'opérations de développement et de maintien des capacités techniques interministérielles décidées en comité de pilotage « CTIM » par le cabinet du Premier ministre ;

- de la mise en place de réseaux effectuée par le ministère de la défense au profit du GIC ;

- des programmes interministériels et des études réalisés par la direction générale pour l'armement dans le domaine de la sécurité des systèmes d'information, notamment le programme de modernisation des produits gouvernementaux de sécurité des communications électroniques (PMPS) et celui de cryptophonie de nouvelle génération (CNG) ;

- de moyens de lutte NRBC ;

- de travaux d'infrastructure pour le GIC ;

- d'investissements au bénéfice du système COMGOUV[1].

Il est également prévu le transfert de 18,2 M€ d'AE et de 5,3 M€ de CP au profit du programme 216 « Conduite et pilotage des politiques de l'intérieur » pour la réalisation d'un centre informatique sécurisé au bénéfice de l'Agence nationale de sécurité des systèmes d'information (ANSSI)[2].

En effet, le SGDSN s'est associé avec le ministère de l'intérieur pour la création d'une salle sécurisée de serveurs informatiques, répondant à des besoins partagés.

Cet investissement nécessite une réhabilitation et une adaptation immobilière pour un coût total évalué à 24,2 M€ TTC. Le SGDSN s'est engagé à financer les trois-quarts de l'opération, soit 18,2 M€. De son côté, le ministère de l'intérieur finance la part restante et assure la maîtrise d'ouvrage par l'intermédiaire de la direction des systèmes d'information et de communication (DSIC). Certaines dépenses complémentaires identifiées par chacune des parties (par exemple l'aménagement informatique intérieur) ont fait l'objet d'un travail d'harmonisation permettant d'envisager des optimisations d'investissement dans le cadre de la consultation.

La phase d'études et de définition du programme de chaque commanditaire est achevée, de même que la notification du marché de maîtrise d'œuvre. Pour engager la phase de travaux dès 2016, avec l'objectif d'une livraison de l'ouvrage début 2018, il est prévu de transférer la contribution du SGDSN relative à l'engagement juridique (18,2 M€ d'AE) et celle liée à la réalisation des travaux en 2016 (5,3 M€). Il convient de préciser que le ministère de l'intérieur affectera les AE à une tranche fonctionnelle.

Enfin, comme en 2015, le SGDSN souhaite apporter son soutien à l'appel à projets du fonds unique interministériel (FUI) pour stimuler l'émergence de projets sur les thématiques de sécurité au sein des pôles de compétitivité et prévoit à ce titre le transfert d'1 M€ en AE=CP vers le programme 192 « Recherche et enseignement supérieur en matière économique et industrielle» du ministère de l'économie, de l'industrie et du numérique.

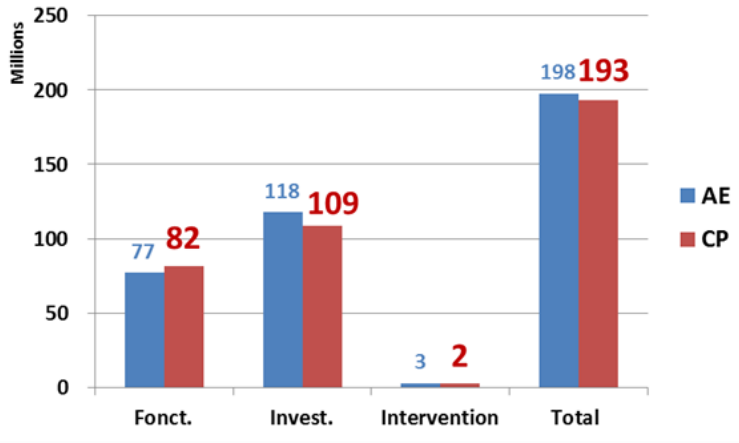
[1] *Ce système permet d'assurer les liaisons de communications sécurisées du Président de la République et du Gouvernement, notamment lors des déplacements par la voie aérienne.*

[2] *Voir supra p.40*

2. Les crédits hors titre 2 en PLF 2017

Le montant total des crédits hors titre 2 s'élève à 197,7 M€ d'AE et 193,1 M€ de CP, dont 16,7 M€ en AE=CP au bénéfice du GIC.

Répartition des crédits par nature de dépense



Source : SGDSN – réponse au questionnaire parlementaire

L'ANSSI représente une part importante des crédits hors titre 2. Les dotations de l'ANSSI. Leur montant dans le projet de loi de finances pour 2017 (66,87 millions d'euros en CP et 72,43 en AE) est stable par rapport à 2016 (67,9 millions d'euros en CP et 73,66 en AE).

Hors ANSSI, le SGDSN dispose de 84,8 millions d'euros en crédits de paiements pour 2017, soit une légère diminution de 4,6 % que l'on retrouve en autorisation d'engagement qui baissent de de 12 % et s'élèvent à 82,82 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 activité, s'élèvent à 11,03 millions d'euros en CP et subissent une érosion sensible (-13%). 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) Crédits de fonctionnement

Les crédits de fonctionnement s'élèvent à périmètre courant (hors GIC) à 68,4 M€ d'AE et 72,9 M€ de CP et sont destinés à couvrir principalement les dépenses et les actions suivantes :

- une enveloppe de 7,6 M€ d'AE et 7,3 M€ de CP sera consacrée aux communications électroniques sécurisées, à la fois dans sa composante réseau et liaisons officielles, ainsi qu'au déploiement et à l'installation d'une boucle optique gouvernementale (1,4 M€ d'AE et 1,7 M€ de CP) et la

maintenance d'un système d'hypervision des systèmes d'information et de communication (SIC) gouvernementaux (1,5 M€ d'AE et 1,3 M€ de CP) ;

- 3,6 M€ en AE=CP seront consacrés aux autres réseaux interministériels pour l'échange d'informations classifiées ou protégées via le réseau IRIS, ainsi que 5,1 M€ d'AE et 5,5 M€ de CP pour couvrir les besoins en produits et services de sécurité au profit de l'ensemble des administrations ;

- l'acquisition de matériels pour les serveurs, postes de travail et matériaux pour les terminaux fixes et mobiles est estimée à 13,1 M€ d'AE et 12,3 M€ de CP ;

- les activités du centre opérationnel de la sécurité des systèmes d'information prévoient 1,8 M€ d'AE et 2,5 M€ de CP pour l'assistance aux victimes d'actes de cyber-malveillance, ainsi que 1,7 M€ et 1,6 M€ de CP pour tout ce qui concerne les techniques opérationnelles d'analyse de la vulnérabilité et les investigations (audits et inspections, systèmes de détection, licences associées aux outils d'analyse de vulnérabilité notamment) ;

- 3,5 M€ d'AE et 3,7 M€ de CP sont provisionnés pour la maintenance et le déploiement de systèmes d'information externes comme Horus, la maintenance applicative ISIS, de ToIP CD, la téléphonie fixe et les « Secdroids » ;

- une enveloppe de 5 M€ en AE et CP aux programmes interministériels de lutte contre la menace nucléaire, radiologique, biologique, chimique et explosive (NRBC-E), ainsi que d'autres programmes liés à la continuité de l'activité de l'État en situation de crise et notamment une participation à l'élaboration du système d'alerte et d'information des populations (SAIP) piloté par le ministère de l'intérieur.

De même, seront pris en charge la réalisation d'exercices nationaux de simulation de gestion de crise et le maintien en conditions opérationnelles des moyens de veille et d'alerte au profit du Gouvernement.

Les autres dépenses de fonctionnement courant sont estimées à 5,5 M€ d'AE et 5,3 M€ de CP et couvriront les frais de mission, de formation, d'action sociale, d'équipement et de mobilier, de documentation ainsi que toutes les dépenses de bureautique non spécifiques.

- S'agissant des dépenses immobilières :

- 5,7 M€ d'AE et 10,4 M€ de CP sont destinés d'une part au paiement du loyer, des charges locatives et des aménagements prévus dans des locaux de l'ANSSI (dont la maintenance des installations techniques et les travaux de continuité de l'installation électrique) et, d'autre part, à l'entretien, à la poursuite de travaux et à l'aménagement de salles de serveurs informatiques ;

- 1,8 M€ d'AE et de CP sont destinés à la prise en charge des travaux de réhabilitation du bâtiment 13 de l'École militaire[1].

Les crédits de fonctionnement permettront également le versement des subventions pour charges de service public des opérateurs placés sous la tutelle du SGDSN à hauteur de 13,8 M€ en AE et CP :

- Institut des hautes études de défense nationale : 7,6 M€ ;
- Institut national des hautes études de la sécurité et de la justice : 6,2 M€.

Conformément à la lettre de cadrage du 27 avril 2016, les mêmes objectifs de réduction des dépenses ont été appliqués aux opérateurs. Ainsi, les subventions pour charges de service public ont été diminuées de 5 % pour les crédits hors personnel.

b) Les dépenses d'investissement

Les crédits d'investissement sont consacrés de façon quasi-exclusive au financement de recherche, de développement et d'acquisition de capacités techniques répondant aux besoins interministériels.

Évalués (hors GIC) à 109,9 M€ d'AE et 101,1 M€ de CP pour 2017, ils ont vocation à financer les projets suivants :

- 22,5 M€ d'AE et 4,4 M€ de CP seront consacrés au développement de logiciels de sécurité nationaux pour la protection des informations classifiées de défense, au travers de programmes conjoints avec le ministère de la défense ;
- 3,9 M€ d'AE et 4,4 M€ de CP seront destinés à l'achat de licences dans le cadre du développement des produits et services de sécurité, et au développement de plateformes dans le cadre de l'expertise scientifique du COSSI de l'ANSSI à destination des opérateurs d'importance vitale et des administrations ;
- 0,3 M€ en AE et CP sont prévus pour le financement de moyens interministériels de défense, notamment l'acquisition de moyens de décontamination NRBC-E, dans le cadre de la convention passée avec le détachement central interministériel d'intervention technique (DCI-IT) ;
- 0,8 M€ d'AE et CP d'achats de matériel sont prévus dans le cadre de la politique de sécurisation des réseaux dont 0,3 M€ en AE et CP pour l'acquisition de chiffreurs, 0,3 M€ d'AE et 0,2 M€ de CP liés au renouvellement d'équipements du système de visio-conférence sécurisé

[1] *Conformément à la convention signée en novembre 2015, le ministère de la défense met à disposition du SGDSN, pour les besoins de l'Institut national des hautes études de sécurité et de justice (INHESJ) et du conseil supérieur de la formation et de la recherche stratégique (CSFRS) des locaux du bâtiment 13, pour une durée minimale de 15 ans à compter du 1er janvier 2016. En contrepartie, le SGDSN participe au financement à hauteur de 60 % du coût de réhabilitation des locaux.*

HORUS et 0,2 M€ en AE et CP d'achats d'oscilloscopes et autre instrumentation spécifique.

- Enfin, 8,5 M€ de CP seront liés à la poursuite de travaux immobiliers (1,1 M€ pour la réfection de la cour extérieure de l'Hôtel National des Invalides[1], 0,7 M€ pour la finalisation de travaux d'amélioration thermique et 6,5 M€ de CP pour le futur centre informatique sécurisé[2]).

- Par ailleurs, une dotation de 82,3 M€ d'AE et 82,7 M€ de CP sera consacrée à des projets interministériels liés à la sécurité nationale. Dans ce processus, le SGDSN attribue les crédits aux services administratifs qui jouent le rôle d'opérateurs techniques; il n'en est pas le bénéficiaire.

c) Les dépenses d'intervention

Le SGDSN a prévu une dotation de 2,8 M€ en AE et 2,5 M€ en CP pour les dépenses d'intervention suivantes :

- 1,1 M€ en AE et en CP sont destinés au fonds unique interministériel (FUI) dans le cadre du cofinancement de projets de recherche innovants, notamment dans le domaine de la protection contre le terrorisme ou la cyber-sécurité ;
- 0,4 M€ en AE et en CP sont attribués dans le cadre de l'appui à différents projets et initiatives dans le domaine de la cyber-sécurité, dont 0,1 M€ en AE et CP dans le cadre de la convention conclue avec Bpifrance, en vue du soutien au développement de produits de sécurité des systèmes d'information ;
- 1,1 M€ en AE et 0,8 M€ en CP sont destinés à des actions de sécurité et de défense, dont 0,03 M€ en AE et CP de subvention au Haut comité français pour la défense civile (HCFDC), et 1,1 M€ d'AE et 0,8 M€ de CP dans le cadre de la convention conclue avec l'Agence nationale de la recherche (ANR) pour des appels à projets liés à la liberté et à la sécurité en Europe ;
- 0,2 M€ en AE et en CP correspondent à la subvention versée au CSFRS.

B. UN EFFORT BUDGÉTAIRE SENSIBLE POUR ACCOMPAGNER LA MONTÉE EN PUISSANCE DU GIC ET L'INTENSIFICATION DE SON ACTIVITÉ

Jusqu'en 2007 inclus, le budget du GIC était abondé uniquement en fonds spéciaux. Une part complémentaire de crédits de droit commun a été

---

[1] Pour répondre, au besoin de réaménagement des locaux de l'Hôtel national des Invalides, afin d'assurer la montée en puissance de l'ANSSI, et aux évolutions de fonctionnement des autres directions le SGDSN a lancé, en octobre 2015, un programme qui s'inscrit dans le cadre du schéma directeur immobilier pluriannuel.

[2] Il convient de rappeler que, conformément à la convention du 9 juillet 2015, 75 % du coût du centre informatique est financé par le SGDSN, le reliquat étant à la charge du ministère de l'intérieur. La totalité des AE à la charge du SGDSN est transférée en gestion 2016. Voir infra p. 40 et 74.

introduite en 2008 à hauteur de 0,4 M€ pour couvrir des dépenses de fonctionnement. Elle a été reconduite jusqu'en 2015 et portée à 0,5 million d'euros en PLF 2016.

	Titre 2	Titre 3	Titre 5	Total HT2	Complément par budget CTIM
LFI 2015 exécutée		0,3		0,3	1,5
PLF 2016	3,9	0,5		0,5	
LFI 2016	4,1			14	1
PLF2017	10,9	8,8	7,8	16,6	

Avec l'évolution des missions confiées au GIC dans la cadre de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement, complétée par la loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, et sauf exception qu'il appartiendra à la commission parlementaire de vérification des fonds spéciaux de contrôler, les dépenses de fonctionnement et d'investissement du GIC peuvent désormais être financées à titre principal par des crédits normaux.

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. Dans la loi de finances pour 2016, ces crédits ont été délégués au SGDSN et portés, après l'adoption d'un amendement du Gouvernement lors de l'examen du projet de loi au Sénat, à 14 millions d'euros (en AE comme en CP). Après prise en compte des éléments de régulation budgétaire, le montant total des crédits disponibles en 2016 s'élève à 11,1 M€ d'AE et de CP.

En 2017, le budget du GIC prévoit un crédit de 16,6 M€ hors titre 2 en autorisations d'engagement et en crédits de paiement dont 8,8 millions de crédits de fonctionnement et 7,8 millions de crédits d'investissements en AE comme en CP, hors CTIM.

1. Les dépenses d'investissement

Les dépenses d'investissement sont essentiellement consacrées à l'achat de licences d'exploitation pour les systèmes informatiques, au règlement d'études de prestations à caractère technique, à l'achat d'équipements techniques spécifiques (serveurs, calculateurs, capacités de stockage, etc.), et aux dépenses d'infrastructure.

Les investissements que réalise le GIC, qu'il s'agisse de dépenses d'infrastructure en raison d'importants travaux liés à la refonte des locaux, comme en 2015 avec la création d'un nouveau centre GIC parisien destiné

aux services d'exploitation du « second cercle », ou des interventions sur les réseaux informatiques et électriques, sont imposés par les évolutions permanentes des technologies des communications électroniques, par les évolutions réglementaires et par les décisions confiant au groupement des missions nouvelles. Si certains projets sont anticipés, la réponse à certains objectifs nécessite une grande réactivité, une forte capacité d'adaptation et une grande souplesse dans la gestion des moyens.

Ces moyens croissants doivent permettre au GIC de mettre en œuvre les missions de la loi sur le renseignement. L'acquisition et le traitement de données supplémentaires se traduiront par l'achat de matériels et la création de systèmes d'information en vue d'exploiter ces données, l'installation de réseaux informatiques et l'aménagement de locaux. L'ensemble de ces installations devront répondre de surcroît à des exigences de sécurité des plus élevées.

En vue de répondre à ses nouvelles missions, le GIC augmentera sa capacité de stockage des données des interceptions de sécurité dont la durée de conservation autorisée passe de 10 à 30 jours, développera des dispositifs d'archivage et de traitement des données recueillies par les techniques de renseignement dont il assure la centralisation, et organisera 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.

En matière de surveillance internationale, la loi dispose que le Premier ministre organise les dispositifs de traçabilité (article L. 854-4 du code de la sécurité intérieure). Une réflexion est en cours sur la possibilité que le GIC, qui participe à la définition et au développement des outils, assure un contrôle permanent de la mise en œuvre et de l'exploitation dans ce domaine.

Afin de faciliter l'accès des services du second cercle aux techniques de renseignement, il est également question de densifier la répartition sur le territoire des centres d'exploitation du GIC.

L'hébergement de ces serveurs de données et des guichets d'exploitation nécessitera également des infrastructures immobilières et en conséquence, l'affectation de surfaces et leur aménagement sur des emprises de l'État. Le GIC devra aussi, pour assurer sa montée en puissance et notamment celle de ses effectifs qui auront à l'horizon 2020 augmenté de près de 40% par rapport à 2016, pourvoir à l'aménagement de ses infrastructures.

2. Les crédits de fonctionnement

Les crédits de fonctionnement courant du GIC, (8,8 millions d'euros), couvriront les dépenses liées aux fluides, à l'achat d'équipements et

de fournitures, ainsi qu'au fonctionnement des centres GIC et du socle informatique et réseau.

Vos Rapporteurs comprennent que la mise en œuvre rapide des dispositions de la loi sur le renseignement impose au GIC avec le soutien du SGDSN une profonde réorganisation de ses modes de fonctionnement budgétaires et financiers. Ils saluent l'orientation définie qui consiste à affranchir le GIC de sa dépendance administrative à la DGSE et à assurer son financement, à titre principal par des crédits généraux. Ils estiment nécessaire que les modalités techniques d'adossement du GIC au SGDSN soient rapidement précisées et arrêtées de façon à entamer la gestion de l'exercice 2017 sur des bases stables. Ils souhaitent qu'à l'avenir, le GIC établisse des règles de gouvernance des crédits qui lui sont dévolus et puissent assurer une programmation pluriannuelle de ses investissements, sans nuire naturellement à la réactivité nécessaire dans un contexte général d'accroissement de ses missions, d'intensification de son activité et de montée en puissance de ses missions.

III. LES FONDS SPÉCIAUX

A. UNE ENVELOPPE DE CRÉDITS EN AUGMENTATION SENSIBLE

Les fonds spéciaux sont consacrés au financement de diverses actions liées à la sécurité extérieure et intérieure de l'État. Ils s'élèvent à 67,8 millions d'euros en autorisations d'engagement et en crédits de paiement dans le projet de loi de finances pour 2017[1] à comparer avec les 47,3 millions d'euros inscrits en loi de finances initiale pour 2016. Ils concernent les services de renseignement et à titre désormais résiduel, le Groupement interministériel de contrôle (GIC). Ces dotations sont souvent majorées en gestion par des décrets pour dépenses accidentelles et imprévisibles.

Dans son premier rapport public sur la gestion des fonds spéciaux, annexé au rapport annuel de la délégation parlementaire au renseignement pour 2015[2], la Commission parlementaire de vérification des fonds spéciaux déplorait l'absence de revalorisation de l'enveloppe consacrée aux fonds spéciaux « *alors que les budgets octroyés aux services de renseignement ont connu une progression appréciable et conforme à la reconnaissance de la fonction stratégique assumée ainsi qu'à la hausse de leur activité (..) alors même qu'ils financent la partie la plus sensible de l'activité de ses administrations* ». Elle s'interrogeait par ailleurs sur « *le recours systématique à des décrets de dépenses accidentelles et imprévisibles (DDAI) afin de financer, au-delà du déclenchement de la crise, des dépenses qui, avec le temps, deviennent prévisibles* » et se demandait

[1] *Source : projet annuel de performance.*
[2] *Rapport de la délégation parlementaire au renseignement pour 2015 p. 101* http://www.senat.fr/rap/r15-423/r15-4231.html

« *en particulier si cette pratique ne constitue pas la contrepartie d'une volonté de maintenir une dotation en fonds spéciaux gelées* ». Enfin, elle attirait *l'attention du Premier ministre sur l'impérieuse nécessité de revaloriser au moins à hauteur de 50% le montant octroyé aux services de renseignement* ».

Dans le projet de loi de finances pour 2017, ces recommandations sont satisfaites.

B. 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 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. Pour la première fois, la CVFS a publié un rapport public en annexe de celui de la Délégation parlementaire au renseignement.

[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.*

TITRE 3 : LES INSTITUTS RATTACHÉS AU SGDSN

Deux opérateurs sont placés sous la tutelle du SGDSN :

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

Les subventions pour charges de service public des deux opérateurs s'élèvent :

- pour l'Institut des hautes études de défense nationale (IHEDN), à 7,6 millions d'euros en AE et en CP (8,1 millions d'euros en LFI 2016) ;

- pour l'Institut national des hautes études de la sécurité et de la justice (INHESJ) à 6,2 millions d'euros en AE et en CP (8,7 millions d'euros en LFI 2016). L'écart constaté tient compte de l'exécution directe, en titre 3, des crédits du SGDSN, des dépenses relatives au bâtiment 13 qui ne sont plus portées par le budget de l'INHESJ opérée en gestion 2016 (1,8 millions d'euros en 2017). Il est vrai que le montage mis en œuvre s'apparentait de fait à un rebasage de la subvention pour charges de service public de l'institut ce qui ne clarifiait guère le pilotage de sa gestion et n'était guère justifié dès lors que le bâtiment devait également héberger la Conseil supérieur de la formation et de la recherche stratégique (CSFRS).

Les crédits de fonctionnement hors personnel prennent en compte les instructions du Premier ministre de baisser de 5 % le montant des subventions pour charge de service public, par rapport à la gestion 2016. La dotation globale destinée aux instituts (IHEDN et INHESJ), ainsi qu'au Conseil supérieur de la formation et de la recherche stratégique (CSFRS), est donc en baisse de 1,2 million d'euros.

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

A. MISSIONS ET ACTIVITÉS DE L'IHEDN

L'Institut des hautes études de défense nationale (IHEDN) a pour mission de développer l'esprit de défense et de sensibiliser aux questions internationales. À ce titre :

- il réunit des responsables de haut niveau appartenant à la fonction publique civile et militaire ainsi qu'aux différentes catégories socio-professionnelles de la nation, des États membres de l'Union européenne ou d'autres États, en vue d'approfondir en commun leurs

connaissances des questions de défense, de politique étrangère, d'armement et d'économie de défense ;

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

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

1. Des orientations formalisées dans un plan stratégique

Ses orientations stratégiques sont aujourd'hui formalisées dans un Plan Stratégique IHEDN 2020[1] adopté en novembre 2015.

Les principales orientations du Plan stratégique IHEDN 2020

Ces orientations stratégiques en phase avec les préoccupations des Français sur la défense du pays, l'étendue et les nouvelles formes de menaces pesant sur la sécurité, les attentes des différents acteurs, les jeunes générations en particulier, concernés par la défense, sont envisagées autour des quatre axes fondamentaux suivants :

- la volonté d'ouverture plus importante en associant un public plus large à ses actions de formation et d'information (féminisation des auditeurs et des intervenants, meilleur équilibre entre fonction publique et secteur privé, attention particulière au monde universitaire et aux enseignants), mais également en développant les actions liées au renforcement de la cohésion nationale (développement d'un second axe de formation consacré au renforcement de la citoyenneté au sein des jeunes générations, ouverture à de nouveaux publics issus de l'enseignement scolaire) ;

- la structuration de la communauté de l'IHEDN, capable de démultiplier l'action, l'influence et la renommée de l'institut ;

- l'information et la transmission de l'esprit de défense, de la connaissance de l'institution militaire, des enjeux de défense, de la pensée stratégique française, par la mise en relation et en réseau de l'ensemble des acteurs publics et privés engagés dans la mission de formation à la défense et à la sécurité globale ; pour l'ensemble de ces raisons, les auditeurs doivent recevoir de l'institut « la capacité à transmettre » ;

- la modernisation et la rationalisation de la gouvernance de l'Institut, par le renforcement de la capacité de pilotage, la rationalisation et la mutualisation des fonctions de soutien, la mise en place des moyens numériques adaptés et d'une infrastructure immobilière restaurée et plus regroupée.

[1] http://issuu.com/ihedn/docs/plan_strat__gique_ihedn_2020_web/1?e=4027381/33785420

2. Un contrat de performance qui tarde à se matérialiser

Si l'IHEDN dispose désormais d'un plan stratégique, elle n'a pas réussi, un an après son adoption, à mettre en place avec l'Etat un contrat de performance comme nombre d'établissements publics, ce contrat permettrait de matérialiser les objectifs soutenus par l'Etat et pour lesquels il apporte, en priorité, des financements publics. Ils constituent un moyen intéressant de pilotage et d'évaluation.

Ces retards induisent un décalage temporel entre la définition de la stratégie et la matérialisation du soutien de l'autorité de tutelle et une difficulté à se mobiliser sur des objectifs clairs.

Vos rapporteurs avaient souhaité dans leur précédent rapport être rendus destinataires du projet afin de pouvoir communiquer, en tant que de besoin, leurs observations, comme peuvent le faire les commissions parlementaires à l'égard des contrats passés par exemple entre le ministère des affaires étrangères et l'Institut français ou Expertise France ou encore l'AFD. Ils renouvellent cette demande.

3. Les objectifs à réaliser en 2017

L'année 2017 s'inscrira dans la continuité de 2016 avec le développement des activités de formation et d'information sur l'esprit de défense nationale.

L'IHEDN va accroître sa présence en région, directement ou par ses relais associatifs, notamment dans le cadre des sessions jeunes qui sont en augmentation sur l'ensemble du territoire. Les actions menées en ce sens, en 2015 et 2016, s'étendront en 2017 en mobilisant le cercle des partenaires à travers le fonds de dotation, et en renforçant les relations de l'IHEDN avec le conseil supérieur de la formation et de la recherche stratégique et l'INHESJ.

L'IHEDN n'est pas un institut de recherche, s'ouvre encore modestement vers l'enseignement universitaire. Il soutient la recherche par la délivrance de prix scientifiques pour des thèses de doctorat et des mémoires de Master 2.

De plus, dans le cadre de sa mission de diffusion de la connaissance et de l'expertise en matière de défense et de politique étrangère, l'IHEDN constate le bilan très positif de la nouvelle session nationale « Enjeux et stratégies maritimes » : l'afflux et la qualité des candidatures encouragent l'institut à organiser une 2e session nationale dès septembre 2016, pour une trentaine d'auditeurs.

L'IHEDN renforce enfin ses relations avec ses partenaires du Conseil supérieur de la formation et de la recherche stratégique (CSFRS) et de l'INHESJ. La mutualisation avec l'INHESJ porte sur le soutien, favorise des synergies pédagogiques, tout en respectant le caractère propre de chaque

institut et permet d'éviter les doublons dans les catalogues de formation, notamment dans le domaine de l'intelligence économique.

Enfin, l'IHEDN poursuit la bascule, depuis le 1er janvier 2016, dans le nouvel environnement du décret relatif à la nouvelle gestion budgétaire et comptable publique et, à ce titre, expérimente le déploiement d'un nouveau système d'information financière. L'application de cette réforme impose une nouvelle organisation pour optimiser le traitement et la maîtrise de la dépense publique. Ce temps d'expérimentation est également un des points de rapprochement et de collaboration entre l'IHEDN et l'INHESJ.

Dans le cadre de la création du groupement comptable unique regroupant les activités comptables de l'IHEDN et de l'INHESJ, approuvé en conseil d'administration de l'IHEDN, le 24 février 2016, des travaux d'aménagement en cours de réalisation vont permettre la colocalisation des personnels des deux établissements.

Si le rapport d'activité de l'IHEDN[1] comprend nombre de données intéressantes sur le nombre et la diversité des formations proposées et réalisées, le nombre des auditeurs et les coûts complets par activités, il ne permet pas, en l'absence d'un critère de mesure homogène, d'apprécier la performance de l'établissement public et l'évolution des coûts par type de session. Il serait souhaitable que celui-ci adopte l'outil traditionnellement utilisé par l'ensemble des organismes de formation, à savoir le volume horaire dédié à chaque formation.

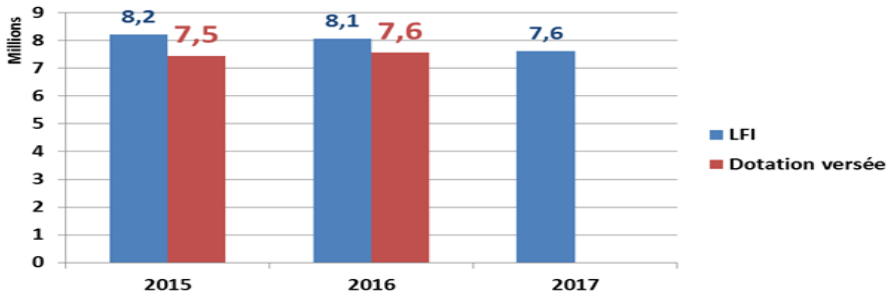
B. L'ÉVOLUTION DES CRÉDITS ET DES EMPLOIS DE L'IHEDN

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

Elle se manifeste par une diminution sensible de la subvention pour charges de service public en loi de finances initiale comme en gestion.

La subvention pour charges de service public a diminué depuis 2013, en loi de finances initiale, et plus encore en gestion, en raison de mise en réserve et de diminution en fin de gestion.

[1] *http://www.ihedn.fr/?q=content/rapport-activite*



Source : SGDSN – réponse au questionnaire parlementaire

En 2015, des efforts ont été demandés sur la partie fonctionnement ainsi que deux emplois au titre de l'effort de productivité. En fin d'année 2015, une modification budgétaire a eu pour objet de prendre en compte la diminution de la subvention pour charges de service public qui est passée de 8,225 millions d'euros en loi de finances initiale pour 2015 à 7,452 millions au compte financier, conformément au schéma de fin de gestion des services du Premier ministre, après application de la mise en réserve de 223 291 euros dès le budget initial, application d'un surgel en cours d'année et d'un prélèvement du fonds de roulement.

Les ressources propres ont compensé cette moindre contribution en progressant de 15,3 % pour atteindre 2,215 millions d'euros, soit 101 000 euros au-delà de la prévision inscrite au budget initial. Ceci est la conséquence de l'effort qui a été engagé depuis 2013 sur la recherche de recettes nouvelles, notamment par une hausse sensible des frais d'inscription, par la sélection d'auditeurs pour lesquels la tarification est la plus élevée (y compris pour les sessions régionales) En revanche, la collecte de la taxe d'apprentissage (51 721 euros) a été moins bénéfique qu'en 2014 (- 37,8 %) en raison de l'évolution de la législation. L'exercice a été soldé en quasi équilibre (+ 22 000 euros) avec un montant de ressources à 9,719 millions d'euros. **Néanmoins, l'instabilité récurrente en cours d'exercice du niveau de la contribution pour charges de service public qui représente 76,7 % des recettes ne permet pas une gestion sereine de l'établissement.**

En 2016, la situation devrait être plus stable avec certes une mise en réserve dès le budget initial de 187 749 € sur une attribution de 8,1 millions d'euros en loi de finances initiale, une attribution de taxe d'apprentissage au même niveau qu'en 2015 et un montant de ressources propres inscrites inférieures à la réalisation 2015. **L'équilibre reposera une nouvelle fois sur la capacité de l'IHEDN à réduire ses dépenses et à collecter des ressources propres avec un budget d'un montant de 10,05 millions d'euros.**

L'année 2016 est marquée également par la mise en application opérationnelle du décret n° 2012-1246 du 7 novembre 2012 relatif à la gestion budgétaire et comptable publique (GBCP) qui concerne l'organisation financière des établissements publics de l'État.

Retenu parmi les 50 organismes pilotes, l'IHEDN a basculé depuis le 1er janvier 2016 dans le nouvel environnement financier et mène le déploiement délicat d'un système d'information financier encore non stabilisé à ce jour. L'application de la réforme financière instaure une comptabilité budgétaire distincte de la comptabilité générale, mais avant tout, des nouvelles organisations visant à optimiser le traitement et la maitrise de la dépense publique.

Cette nouvelle orientation est également un des points de rapprochement et de collaboration entre l'IHEDN, pilote, et l'INHESJ.

Le montant de la subvention annoncée pour 2017 est de 7,615 millions d'euros. L'IHEDN supporte une diminution de 5 % de ses crédits de fonctionnement par rapport à 2016 ; en outre, deux emplois seront supprimés, le nombre d'ETPT autorisé revenant à 92. Trois autres emplois en fonction au sein de l'IHEDN sont rémunérés par d'autres programmes en PLF 2017, soit le même nombre qu'en LFI 2016. Ces emplois sont ainsi mis à disposition à titre gracieux par le ministère de la défense, le ministère des affaires étrangères et du développement international et par le ministère de l'intérieur.

Ces diminutions successives du plafond d'emploi ont naturellement une limite. En fait, l'IHEDN devra opérer désormais une mutation dans son organisation pour transformer sa structure d'emploi et l'adapter à ses nouvelles orientations stratégiques. Elle pourrait poursuivre la politique de dépyramidage afin de recruter des emplois au plus près du cœur de métier de jeunes experts et autres spécialistes.

L'IHEDN bénéficie en outre du soutien logistique du ministère de la défense pour l'organisation, notamment, de déplacements et de présentations.

Ce soutien constitue une forme de contrepartie à la formation que reçoivent les militaires au sein de l'Institut, notamment ceux du Centre des hautes études militaires (CHEM) qui sont parallèlement auditeurs de la session nationale. Cependant, les contraintes, qui pèsent sur les Armées en raison de leur fort engagement en OPEX et sur le territoire national, impactent désormais les capacités d'organisation des sessions de l'IHEDN et ses coûts de fonctionnement[1].

L'équation budgétaire demeurera donc, comme lors des précédents exercices, sous tension : l'IHEDN devra trouver à faire progresser ses **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**.

L'accroissement des missions dans un cadre budgétaire très contraint a sans doute pour principal vertu d'obliger les dirigeants à se montrer plus rigoureux dans l'affectation des moyens aux missions et de

[1] *Notamment, l'indisponibilité fréquente des moyens de transports aériens.*

favoriser des économies de structure. L'IHEDN est confronté depuis plusieurs années à cette difficulté. Reste que, pour assurer sa transformation, il lui faut pouvoir transformer des emplois de généralistes, parfois anciens, en des emplois de profils plus spécialisés et plus jeunes pour mener les missions nouvelles et recueillir des financements. Ce n'est pas très simple lorsque les marges de manœuvre budgétaires sont réduites et sans avoir pu conclure un contrat de performance avec l'Etat qui, d'un côté, est prompt à diversifier les missions de l'Institut et qui, de l'autre, n'est pas en mesure de lui donner les moyens de les mettre en œuvre.

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 arrêtées en novembre 2015 puissent être traduites dans un contrat de performance entre l'État et l'établissement.

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

Créé en 1989, l'INHESJ est l'opérateur public de référence dans les domaines de la formation et de la recherche liés à la sécurité globale et à la justice.

Sa spécificité est d'être un espace orienté vers l'identification pluridisciplinaire de l'évolution des champs de la sécurité et de la justice. Conformément aux objectifs de création de l'INHESJ, les formations affirment les liens de la justice et du droit avec les questions de sécurité, mais également de défense. Cela permet à l'INHESJ de préparer les cadres des secteurs publics et privés à l'exercice de leurs responsabilités en application du Livre blanc sur la défense et la sécurité nationale.

Il accueille également, en son sein, l'Observatoire national de la délinquance et des réponses pénales (ONDRP) qui est l'un de ses départements. Les travaux de l'ONDRP sont réalisés avec l'appui de l'INSEE et font l'objet de plusieurs publications dont un rapport annuel sur la criminalité en France.

A. MISSIONS ET ACTIVITÉS DE L'INHESJ

Les missions de l'institut, inscrites dans le code de la sécurité intérieure, répondent à la volonté exprimée au sommet de l'État d'adopter une approche globale dans l'identification des risques et des menaces, comme dans la réponse qu'il convient de leur apporter, en combinant les moyens de la formation et de la connaissance.

1. Des missions formalisées dans un plan stratégique

Le plan stratégique de l'INHESJ 2015-2017[1], adopté en mars 2015 par son conseil d'administration, porte l'ambition de l'institut d'être l'opérateur de référence dans ses missions fondatrices. 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 par le conseil d'administration de l'INHESJ :

- prendre en compte de façon transversale la dimension « justice » 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.

2. Le contrat d'objectifs et de performance : un outil de pilotage sous-utilisé

Afin de renforcer la dimension stratégique, **un contrat d'objectifs et de performance (COP) a été signé le 18 mai 2016**, après avis favorable du conseil d'administration donné en mars 2015. Il reprend les objectifs stratégiques et les complète par des objectifs intermédiaires et par des indicateurs comme par exemple le nombre d'heures de formation délivrées, le nombre de personnes formées, le taux de satisfaction des formations et le taux de renouvellement des intervenants. Il intègre les objectifs partagés de mutualisation avec l'IHEDN.

Par principe, vos rapporteurs s'étonnent de la longueur de la procédure, le COP aurait dû être adopté dans la foulée du plan stratégique dont il constitue une déclinaison et pour la même durée, pour être un outil efficace de pilotage de l'établissement. Signé en mai 2016, il ne s'appliquera que sur la moitié de la période considérée, soit 18 mois…

Ces retards ne permettent pas aux rapporteurs de disposer du suivi des indicateurs de performance adossé au COP pour 2015. Néanmoins, l'INHESJ a communiqué à vos rapporteurs un état d'avancement du plan

[1] *https://www.inhesj.fr/sites/default/files/fichiers_site/inhesj/plan_strategique_inhesj.pdf*

stratégique qui permet de mesurer sa mise en œuvre. Ce document est présenté comme une annexe au rapport annuel d'activité[1].

Vos rapporteurs engagent la nouvelle direction de l'INHESJ, et sa tutelle a engagé très rapidement, en 2017, la réflexion sur l'évolution du plan stratégique et, parallèlement, sur le prochain COP. Ils souhaiteraient également que l'on reconsidère la durée de vie de ces documents, une période effective de 4 ou 5 ans serait plus judicieuse pour programmer le développement de cet établissement. Enfin, ils réitèrent leur demande que les COP soient transmis pour avis aux commissions parlementaires compétentes.

3. Quelques aspects des activités en 2016

Sur le plan immobilier, l'institut a déménagé en février 2016 dans un bâtiment entièrement rénové au sein de l'Ecole militaire, après cinq années passées dans des locaux provisoires. Ce bâtiment héberge un nouveau plateau de formation à la gestion de crise équipé des technologies de pointe en la matière. Cette occupation se traduit par la fin du bail d'occupation de l'immeuble que l'INHESJ occupe à Saint-Denis.

La situation immobilière de l'INHESJ se limitera, donc, à compter de 2017, à l'occupation d'une partie du bâtiment 13 de l'École militaire.

Enfin, à l'instar de l'IHEDN, aucune dépense de l'institut n'a été prévue pour financer des projets de recherche ou d'études confiés à d'autres organismes. A l'inverse, l'INHESJ, qui a renforcé en 2015 son équipe de chercheurs (passée de 4 à 6), répond lui-même régulièrement à des appels à projets ou commandes publiques, et recherche des financements extérieurs pour consolider ses propres projets. Des démarches en ce sens sont par exemple engagées auprès de l'Agence nationale de la recherche, la MILDECA, le Centre de recherche et de formation à la recherche stratégique et la Commission européenne, etc.

4. Les objectifs à réaliser en 2017

Pour 2017, sont prévues des formations spécifiquement dédiées aux cadres dirigeants du ministère de la culture, aux nouveaux ambassadeurs, aux recteurs et à leurs équipes, ainsi qu'aux élus et à leurs collaborateurs et attachés parlementaires. L'activité de formation du département « Risques et crises » connaît une hausse exponentielle depuis les attentats terroristes et suscitent également une demande de l'étranger

Par ailleurs, des séminaires portant sur la radicalisation djihadiste, regroupant préfets, recteurs et procureurs, seront organisés en partenariat

[1] *Toutefois, il n'est pas publié sur le site internet de l'INHESJ en annexe à ce rapport* https://www.inhesj.fr/sites/default/files/fichiers_site/inhesj/ra_2015.pdf

avec le Comité interministériel de prévention de la délinquance et de la radicalisation (CIPDR).

Enfin, une nouvelle session sur les risques aéroportuaires destinée aux sous-préfets et aux administrateurs civils est prévue.

B. L'ÉVOLUTION DES CRÉDITS ET DES EMPLOIS DE L'INHESJ

La subvention pour charges de service public de l'Institut national des hautes études de la sécurité et de la justice (INHESJ) inscrite au programme 129 pour 2017 s'élève à 6,2 millions d'euros en AE et en CP contre 8,7 millions d'euros en LFI 2016.

L'écart constaté tient compte :

- **d'une part, de l'exécution directe en titre 3 des crédits du SGDSN des dépenses relatives au bâtiment 13 qui ne sont plus portées par le budget de l'INHESJ, à la suite d'une modification intervenue en gestion 2016 (1,8 million d'euros en 2017)[1].** Une convention de financement des travaux de réhabilitation du bâtiment 13 a été signée le 13 novembre 2015. Elle prévoit que le ministère de la défense met des locaux à disposition de l'INHESJ, notamment en contrepartie d'une participation au financement de la réhabilitation. Cette dépense est désormais prise en charge par le SGDSN directement, ce qui permettra un meilleur pilotage de la gestion budgétaire de l'INHESJ.

- **d'autre part, des économies demandées par le Premier ministre avec une** baisse de 5 % du montant de subvention pour charge de service public ainsi rebasée, par rapport à la gestion 2016.

La baisse de la dotation budgétaire devra être compensée par l'augmentation des ressources propres et par des prélèvements opérés sur le fonds de roulement.

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.

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

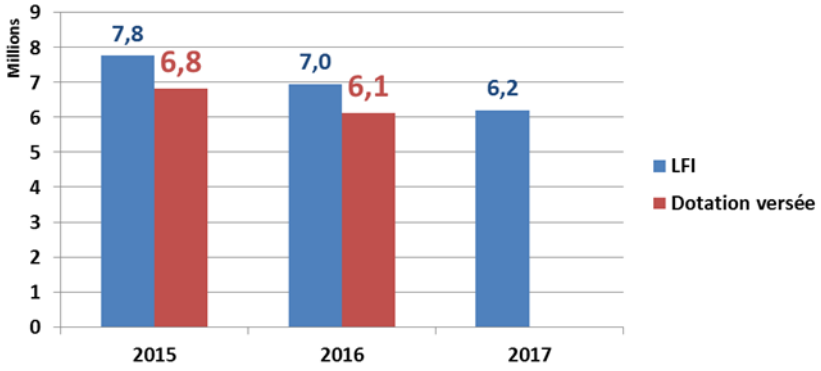
---

[1] *Le montage mis en œuvre jusqu'alors permettait d'affecter aux financements des travaux de réaménagement du bâtiment 13 de l'École militaire, le produit des loyers obtenus de sous-locataire de l'immeuble de Saint-Denis, occupé précédemment par l'Institut et dont le bail ne pouvait être résilié avant le terme. Il s'apparentait, de fait, à un rebasage de la subvention pour charges de service public ce qui ne clarifiait guère le pilotage de sa gestion et n'était plus guère justifié dès lors que le bâtiment devait également héberger le Conseil supérieur de la formation et de la recherche stratégique (CSFRS).*

Elle se manifeste par une diminution sensible de la subvention pour charges de service public en loi de finances initiale comme en gestion.

La subvention pour charges de service public a diminué depuis 2013, en loi de finances initiale et plus encore en gestion, en raison de mise en réserve et de diminution en fin de gestion.

La subvention de l'INHESJ, nette du financement du bâtiment 13 de l'École militaire, est en baisse sensible en loi de finances initiale, mais également en gestion en raison des mises en réserves et des diminutions en fin d'exercice.



Source : SGDSN – réponse au questionnaire parlementaire

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 million d'euros au titre de la contribution à l'opération immobilière susvisée. En gestion, le compte financier fait apparaître, à hauteur de 11,04 millions d'euros, un résultat bénéficiaire de 0,7 million d'euros en raison d'une progression des ressources propres qui passent de 3,5 millions d'euros en 2014 à 4,2 en 2015[1] malgré la perte du bénéfice de la taxe d'apprentissage, et une baisse sensible des charges de personnel (6,1 millions d'euros contre 6,7 en 2014).

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[2] 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

[1] *Y compris les recettes destinées au financement du bâtiment 13 de l'École militaire à hauteur de 1,7 million d'euros*

[2] *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.*

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 6,7 millions d'euros. L'écart constaté entre la subvention pour charge de service public prévu en LFI 2016 et celui prévu dans le cadre du budget initial 2016 de l'INHESJ est dû principalement aux dépenses relatives au bâtiment 13, finalement exécutées en titre 3, à la mise en réserve d'une partie des crédits et à des mesures de régulation budgétaire. 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.

Le budget initial 2016, validé par le conseil d'administration, s'établissait à 8,2 M€. Toutefois, la subvention pour charges de service public 2016 (6 664 715 € dans le budget initial) a été minorée de 533 333 € dans le cadre du décret n° 2016-732 du 2 juin 2016 portant annulation de crédits à titre d'avance au titre du budget 2016. Elle s'établit donc à 6 131 382 €. Cette modification donnera lieu au vote d'un budget rectificatif.

Le financement du nouveau plateau de simulation de gestion de crise a fait l'objet d'un prélèvement sur le fonds de roulement en 2016 à hauteur de 557 000 euros.

En 2017, après signature de la convention du 13 novembre 2015, la subvention pour charges de service public, qui n'intègre plus le financement du bâtiment 13 (1 789 763 € à partir de 2016), est établie à 6 205 450 €.

Les emplois rémunérés par l'opérateur en 2017 sont de 73 ETPT contre 77 ETPT en LFI 2016, soit une diminution de 4 ETPT. Dans le cadre du PLF 2017, tous les emplois sont rémunérés par l'opérateur alors que 7 autres emplois en fonction au sein de l'INHESJ n'étaient pas rémunérés par le programme 129 en LFI 2016.

L'année 2017 devrait permettre à l'Institut de rattraper son retard en matière de modernisation des outils informatiques : un prélèvement sera ainsi opéré sur le fonds de roulement, pour un montant en cours de consolidation. L'utilisation du fonds de roulement, dont le niveau est suffisant pour la réalisation d'investissements, est aujourd'hui judicieuse.

L'institut envisage de mieux structurer son contrôle de gestion, grâce à la mise en place d'une comptabilité analytique. La modernisation du progiciel financier, rendue nécessaire par l'instauration de la nouvelle gestion budgétaire et comptable publique (GBCP), va sans aucun doute permettre une meilleure évaluation, un suivi « en temps réel » des dépenses de fonctionnement et, par conséquent, une plus grande rationalisation de ces dernières. Un travail important sur les marchés publics permettra également de répondre aux attentes de rationalisation des dépenses.

Vos rapporteurs saluent ce retour à une plus grande sincérité budgétaire qui facilitera le pilotage de la gestion de l'INHESJ au service des orientations défini dans le plan stratégique et des objectifs du contrat d'objectifs et de performance. Il devra à l'avenir, pour dégager des marges de manœuvre, développer ses ressources propres et poursuivre sa politique de réduction des coûts de personnel, en faisant évoluer sa structure d'emploi comme il a commencé à le faire (dépyramidage, emploi de jeunes experts et de profils plus spécialisés) et de fonctionnement, notamment par le rapprochement et la mutualisation engagés avec l'IHEDN.

III. 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 création de l'agence comptable unique regroupant les activités comptables de l'IHEDN et de l'INHESJ a été inscrite à l'ordre du jour des conseils d'administration des deux opérateurs en début d'année 2016.

Une convention tripartite constitutive du groupement a été signée le 6 avril 2016, pour une date d'effet au 1er janvier 2016.

Actuellement, des travaux d'aménagement sont en cours de réalisation au sein du bâtiment 10 de l'École militaire, pour permettre le regroupement et l'accueil des personnels mis à disposition par chaque établissement.

Enfin, l'expérimentation par l'IHEDN du déploiement d'un nouveau système d'information financière, dans le cadre du décret relatif à la nouvelle gestion budgétaire et comptable publique et qui impose une nouvelle organisation pour optimiser le traitement et la maîtrise de la dépense publique, est également un des points de rapprochement et de collaboration entre l'IHEDN et l'INHESJ.

- 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 est l'un des axes des plans stratégiques des contrats de performance qui sont et seront présentés et approuvés depuis 2015.

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.

Ils estiment enfin nécessaire de faire coïncider davantage les démarches stratégiques et contractuelles des deux Instituts. S'ils doivent poursuivre la mutualisation de leurs moyens et la mise en cohérence de leurs missions, il serait hautement souhaitable que les plans stratégiques et les contrats de performance portent sur la même période et que les dirigeants de chacun des deux Instituts associent leurs homologues respectifs à la démarche stratégique conduite au sein de leur établissement. Les décalages calendaires dans la mise au point de ces documents entraînent nécessairement des évolutions, voire des contradictions, qui rendent plus difficiles la mise en œuvre des plan et contrat intervenus les premiers ou la réalisation des synergies. Cela aurait pu être l'occasion en 2016, puisqu'après avoir adopté son plan stratégique en mars 2015, l'INHESJ concluait un contrat d'objectifs et de performance en mai 2016. **Puisque le contrat en vigueur de l'INHESJ s'achève en 2017 et que celui en cours de négociation par l'IHEDN devait couvrir la période… 2015-2017, l'opportunité est offerte aux deux instituts de travailler de conserve et sous l'autorité du SGDSN, à la mise au point de contrats couvrant la période 2018-2020.**

TITRE 4 : L'ACADÉMIE DU RENSEIGNEMENT

La création de l'Académie du renseignement, en 2010[1], 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[2] »**.

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 total de stagiaires, leur répartition par formation comme leur identité, sont couverts par le secret de la défense nationale. Toutefois, **plusieurs milliers de personnes ont été formés** par l'académie depuis sa création.

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 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 quatorze personnes dont la directrice, son adjointe, et 5 conseillers pédagogiques[3].

Ses crédits sont gérés par les services du Premier ministre (action n° 01 « coordination du travail gouvernemental ») du programme 129.

	Exécution 2014	Exécution 2015	Exécution au 31 juillet 2016
Titre 2 (en €)	967 981	926 547	658 317
Hors titre 2 (en €)	262 414	237 571	115 736
Total (en €)	1 230 395	1 164 118	774 053
Plafond d'emplois (en ETPT)	9,7	10,2	13

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

[2] *Comprenant, autour du Coordonnateur national du renseignement, six services (DGSE, DGSI, DRM, DPSD, DNRED et TRACFIN). Le décret n° 2014-274 du 12 mai 2014 formalise cette appartenance.*

[3] *L'effectif cible de l'académie du renseignement est de 15 ETP au 31 décembre 2016.*

L'académie du renseignement dispose d'une enveloppe de crédits de fonctionnement déterminée dans le cadre d'un dialogue de gestion avec la direction des services administratifs et financiers du Premier ministre. Pour 2017, l'enveloppe sera déterminée en décembre à la suite du dialogue de gestion annuel.

Son budget exécuté de fonctionnement s'élevait en 2015 à 237 571 euros (262 414 en 2014, - 9,46%). Les crédits de personnel représentaient quant à eux **926 574 euros (967 981 en 2014, - 4,28%). Cette sobriété budgétaire est à saluer, dans un contexte où les missions de l'Académie ont monté en puissance à rythme soutenu.**

En raison des nombreux recrutements dans l'ensemble des services de renseignement, d'une demande forte et légitime d'une partie des services dits du « second cercle » - notamment la direction de l'administration pénitentiaire (DAP), la direction du renseignement de la préfecture de police de Paris (DRPP), le service central du renseignement territorial (SCRT) et la sous-direction de l'anticipation opérationnelle (SDAO) - en direction de l'académie, mais aussi de la nécessaire ouverture de l'académie au monde universitaire et de la recherche, le format de l'académie et la diversification des profils de ses personnels devront faire l'objet d'une réflexion.

En loi de finances pour 2016, ces crédits de fonctionnement ont été portés à 355 000 euros.

À l'initiative de l'académie, le prochain comité d'orientation et d'évaluation devrait valider un plan stratégique qui détaillera les orientations de l'académie pour les années à venir. **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 16 novembre 2016.

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

M. Yves Pozzo di Borgo. – Vous avez fait état du montant des fonds spéciaux. Ils sont couverts par le secret de la défense nationale. Savez-vous si l'ANSSI en bénéficie ?

M. Jean-Pierre Masseret, rapporteur pour avis. **–** Le montant est connu puisqu'il figure dans le programme annuel de performance annexé au projet de loi de finances. Ils sont destinés au financement d'actions liées à la sécurité extérieure et intérieure de l'Etat. Leur affectation est couverte par le secret de la défense nationale. Il appartient à une instance parlementaire spécifique, la commission de vérification des fonds spéciaux, d'en contrôler l'utilisation.

M. Jean-Marie Bockel, rapporteur pour avis. – Nos capacités de cyberdéfense, sous tous leurs aspects, participent à la souveraineté de la France. Ces capacités sont reconnues sur le plan international.

M. Robert del Picchia. – Les autres pays européens font-ils un effort équivalent ? Comment se situe la France en Europe en matière de cyberdéfense ? Les Européens coopèrent-ils ?

M. Jean-Pierre Masseret, rapporteur pour avis. – Il existe une coopération entre les pays européens.

M. Jean-Marie Bockel, rapporteur pour avis. – S'il y a quelques années la France était un peu en retard sur ces questions, ce n'est plus le cas depuis la création de l'ANSSI. Les autres pays comme la Grande-Bretagne ou l'Allemagne ont des organismes dédiés à la cyberdéfense et y affectent des moyens au moins équivalents à ceux de l'ANSSI. Ils sont d'ailleurs en train de réévaluer à la hausse ces moyens et ils ont raison, car dans un domaine où les technologies évoluent très rapidement, ralentir l'effort, c'est se rendre plus vulnérable. Même de plus petits États comme les Pays-Bas investissent dans ce domaine, sans parler de l'exemple connu de l'Estonie qui, après de violentes cyberattaques peu après son indépendance, a fait de la cybersécurité une priorité et a développé une expertise d'excellence en ce domaine.

S'agissant de la coopération, il s'agit d'un domaine stratégique et donc les partenariats se nouent entre Etats. Au niveau de l'Union européenne, l'élaboration d'une réglementation commune progresse et il existe aussi des financements pour la recherche et le développement.

Mme Nathalie Goulet. – Ma question portait sur le même sujet de la coopération internationale, il y a été répondu.

M. Jean-Marie Bockel, rapporteur pour avis. – La coopération européenne progresse, il y a une vraie prise de conscience. Elle a également progressé au sein de l'OTAN.

La Commission a donné un avis favorable, à l'unanimité, à l'adoption des crédits de la mission « Direction de l'action du gouvernement ».

ANNEXE –
LISTE DES AUDITIONNÉS

➢ **Audition en commission plénière :**

- Mercredi 19 octobre 2016 :

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/20161017/etr.html#toc4

➢ **Auditions par les rapporteurs :**

- Mardi 4 octobre 2016 :

M. Cyrille Schott, directeur de l'INHESJ

suivie d'une visite dans les locaux de l'INHESJ dans l'enceinte de l'Ecole Militaire (le jeudi 27 octobre 2016)

- Mercredi 5 octobre 2016 :

M. le Général de Courrèges d'Ustou, directeur de l'IHEDN

- Mardi 11 octobre 2016 :

M. Pascal Chauve, directeur du GIC