N° 110

SÉNAT

SESSION ORDINAIRE DE 2017-2018

Enregistré à la Présidence du Sénat le 23 novembre 2017

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* **2018**, *ADOPTÉ PAR L'ASSEMBLÉE NATIONALE,*

TOME IX

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

Par MM. Olivier CADIC et Rachel MAZUIR,

Sénateurs

(1) Cette commission est composée de : M. Christian Cambon, *président ;* MM. Pascal Allizard, Bernard Cazeau, Mme Hélène Conway-Mouret, MM. Robert del Picchia, Thierry Foucaud, Mme Sylvie Goy-Chavent, MM. Jean-Noël Guérini, Joël Guerriau, Cédric Perrin, Gilbert Roger, *vice-présidents ;* M. Olivier Cigolotti, Mme Joëlle Garriaud-Maylam, MM. Philippe Paul, Rachid Temal, *secrétaires ;* MM. Jean-Marie Bockel, Gilbert Bouchet, Michel Boutant, Olivier Cadic, Alain Cazabonne, Pierre Charon, Édouard Courtial, René Danesi, Gilbert-Luc Devinaz, Jean-Paul Émorine, Bernard Fournier, Jean-Pierre Grand, Claude Haut, Mme Gisèle Jourda, MM. Jean-Louis Lagourgue, Robert Laufoaulu, Ronan Le Gleut, Jacques Le Nay, Rachel Mazuir, François Patriat, Mme Marie-Françoise Perol-Dumont, MM. Gérard Poadja, Ladislas Poniatowski, Mmes Christine Prunaud, Isabelle Raimond-Pavero, MM. Stéphane Ravier, Hugues Saury, Bruno Sido, Jean-Marc Todeschini, Raymond Vall, André Vallini, Yannick Vaugrenard, Jean-Pierre Vial, Richard Yung.

Voir les numéros :

Assemblée nationale (**15**ème législ.) : **235**, **264** ***rect.***, **266** ***rect.***, **273** à **278**, **345** et T.A. **33**

Sénat : **107** à **109** et **111** à **114** (2017-2018)

S O M M A I R E

LES PRINCIPALES OBSERVATIONS

1. La demande de crédits inscrite dans le projet de loi de finances pour 2018 dans le programme 129 « Coordination du travail gouvernemental » est de 685,13 M€, soit 42,6 % 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 **352,01 M€** (347,93 en 2017) en autorisations d'engagement et de **353,73 M€** de crédits de paiement (343,33 en 2017). Par rapport à la prévision inscrite en loi de finances initiale pour 2017, la dotation de cette action enregistre une **croissance de 3,03** % en CP **+10,4 M€**) comme en autorisations d'engagement (+1,17%, 4,083 M€) en raison de la poursuite de la montée en puissance de l'ANSSI et du GIC.

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 près de 60% des effectifs budgétaires et plus de 40% des crédits de l'unité opérationnelle SGDSN (opérateurs compris).

Vos rapporteurs regrettent que les crédits de l'ANSSI ne fassent pas l'objet d'une présentation distincte dans le PAP. Ce serait un moyen de distinguer les efforts en matière de cyberdéfense et les moyens dévolus aux autres missions du SGDSN. Ils demandent que la maquette de présentation du programme soit modifiée dans ce sens.

2.1. Les effectifs du SGDSN (hors ANSSI) restent stables. Le surcroît d'activité sera absorbé par des gains de productivité.

2.2 **La poursuite des créations d'emplois au sein l'ANSSI est confirmée**. Ses effectifs devraient s'accroître de 25 ETP et atteindre 675 ETP en 2022.

Les problèmes de recrutement rencontrés par l'ANSSI lors de sa phase de montée en puissance sont largement résolus. Néanmoins une attention vigilante doit être maintenue. Le vivier de formation initiale reste faible au regard des besoins et le ralentissement de créations de postes ne paraît guère cohérent avec le développement probable des missions de l'ANSSI pour faire face à une menace croissante. Vos rapporteurs espèrent que la Revue de la stratégie cyber en cours sous la direction du SGDSN constituera un levier pour apporter plus rapidement à l'ANSSI les moyens nécessaires à l'exécution de ses missions.

Au-delà de la politique de labellisation des filières de formation par l'Agence, une politique active de développement de filières de formation initiale par une implication plus forte du ministère de la recherche et de l'enseignement supérieur et des partenaires économiques, est indispensable.

2.3. 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 2018 un transfert **6 M€ en CP** pour la réalisation de ce projet dont le ministère de l'intérieur est le maître d'ouvrage.

2.4. Trois ans après la publication de la circulaire du Premier ministre du 17 juillet 2014 exposant la « ***Politique de sécurité des systèmes d'information de l'État*** » (PSSIE) et des règles de protection, **le niveau effectif de conformité des systèmes d'information de l'État tarde à atteindre des niveaux en adéquation avec les enjeux.** Le comblement de ce retard souffre l'insuffisance des moyens organisationnels et budgétaires. Le service interministériel de supervision se heurte à des contraintes techniques et d'organisation qui ne permettent pas toujours de déployer ses sondes sur les réseaux dans des conditions adéquates, ni de recueillir toutes les informations nécessaires pour assurer une détection optimale.

Cette situation reste insatisfaisante au regard des objectifs de conformité complète à la PSSIE. Pour la deuxième année, vos rapporteurs s'inquiètent de la lenteur du processus. Ils attirent l'attention du Premier ministre sur l'acuité de la menace (cf les attaques en 2017 contre le service de santé britannique) et lui demandent de sensibiliser avec fermeté l'ensemble des ministres, seuls les ministères de la défense et de l'intérieur ont produits les efforts nécessaires. Ils demandent qu'une évaluation soit conduite par un corps d'inspection en vue d'identifier les difficultés et de proposer un plan d'actions destinées à accélérer la mise en œuvre de ces dispositions par les ministères concernés. Ils souhaitent que soient étudiés rapidement les moyens juridiques et techniques permettant à l'ANSSI de disposer de moyens de contraintes pour imposer ses préconisations aux directions des systèmes d'information des ministères.

3. Les subventions destinées à l'IHEDN et à l'INHESJ sont maintenues à hauteur de 13,8 M€, soit un montant identique à celui inscrit dans la loi de finances pour 2017, après plusieurs années de diminution. Ceci devrait constituer un socle permettant le développement de leurs activités, notamment celles susceptibles de produire des ressources propres. **Vos Rapporteurs relèvent que le plafonnement des emplois constitue un frein au développement à la réalisation de cet objectif et souhaitent son assouplissement. La mutualisation des moyens et le développement de synergies entre les deux établissements désormais installés sur le site de l'École militaire restent des objectifs à parfaire**.

Vos rapporteurs s'étonnent du retard pris dans la rédaction du contrat d'objectifs et de performance de l'IHEDN. Ils saluent la démarche de l'INHESJ qui aura mené de front, en 2017, la rédaction d'un nouveau plan stratégique et la négociation d'un contrat d'objectifs et de performance avec l'Etat. Ils estiment nécessaire de faire coïncider davantage les démarches stratégiques et contractuelles des deux Instituts.

4. Les fonds spéciaux s'élèvent à 67,4 M€, soit un montant légèrement inférieur à celui inscrit dans le projet de loi de finances pour 2017. **Cette légère diminution, après un ajustement sensible en 2017, est préoccupante** car leur progression devrait accompagner la montée en puissance des services de renseignement fortement sollicités dans le cadre de la lutte contre le terrorisme. Vos rapporteurs restent perplexes. La revalorisation du montant de ces fonds opérés en 2017 aurait dû se poursuivre, l'exercice précédent de « sincérisation » ne constituant qu'une partielle remise à niveau.

5. Pour l'application de la loi de 2015, l**e Groupement interministériel de contrôle (GIC)** est devenu le pivot interministériel de gestion de l'ensemble des techniques de renseignement. L'usage de nouvelles techniques, notamment dans la lutte contre le terrorisme, entraîne une intensification significative de son activité. Il doit en conséquence poursuivre sa transformation et sa montée en puissance.

La révision du statut d'ensemble de son personnel est intervenue en 2017. Au total, les effectifs du GIC devraient atteindre 200 ETP fin 2017 et s'accroître de 15 ETP en 2018, pour atteindre 243 TP en 2020. Votre Commission, comme la DPR, avaient attiré l'attention du Premier ministre sur la nécessité de veiller au bon dimensionnement du GIC pour une mise en œuvre efficace de la loi.

Un effort budgétaire est réalisé pour accompagner sa montée en puissance. Les crédits hors titre 2 sont maintenus à un niveau important de 15,61 M€ (16,6 M€ en 2017), dont les trois quarts pour des investissements.

Vos rapporteurs souhaitent que le Premier ministre continue à se montrer particulièrement attentif à la montée en puissance rapide du GIC.

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 2018.*

Mesdames, Messieurs,

L'examen des crédits du programme 129 « Coordination du travail gouvernemental » de la mission « Direction de l'action du Gouvernement », donne l'occasion à votre commission de se pencher plus attentivement sur les crédits inscrits à l'action 2 « Coordination de la sécurité et de la défense ».

CRÉDITS DE L'ACTION 2 DANS LE PROGRAMME 129

	Autorisations d'engagement (M€)	Crédits de paiement (M€)	Plafond d'emploi (ETPT)
P129	685,13	713,25	1 191
ACTION 2	352,01	353,73	2 991
RATIO ACTION2/P129	51,38%	49,54%	39,82

Sources : PLF2018

Au total, environ la moitié du programme 129 est directement consacrée à des actions touchant la sécurité nationale et la défense. L'**action 2** est dotée dans le projet de loi de finances pour 2018 de **352,01 M€** (en autorisations d'engagement (AE) et **353,73 M€** de crédits de paiement (CP).

Ces crédits progressent de 1,2% en AE et de 3% en CP

CRÉDITS DE L'ACTION 2 « COORDINATION DE LA SÉCURITÉ ET DE LA DÉFENSE »

		Titre 2	Hors titre 2	**Total**
Autorisations d'engagement	2018	89 613 387	262 395 987	**352 009 374**
	2017	84 467 059	265 533 340	**350 000 399**
	2016	70 907 605	256 407 513	**327 315 118**
	2015	*61 995 478*	*165 383 576*	***227 379 054***
Crédits de paiement	2018	89 613 387	264 119 934	**353 733 321**
	2017	84 467 059	260 936 845	**345 403 904**
	2016	70 907 605	244 381 062	**315 288 667**
	2015	*61 995 478*	*173 957 584*	***235 953 062***

En euros.
Sources : 2015 autorisations et crédits consommés (rapport annuel de performances/loi de règlement), 2016 2017 : Projet annuel de performances/ projet de loi de finance, PLF 2017 & 2018.

RÉPARTITION PAR SOUS-ACTIONS DES CRÉDITS DE L'ACTION 2

	PLF 2017		PLF 2018	
	AE	*CP*	*AE*	*CP*
SGDSN	***254 629 749***	***250 033 254***	***256 460 516***	***258 184 463***
Titre2	73 560 211	73 560 211	77 054 258	77 054 258
Hors titre 2	181 069 538	176 473 043	179 406 258	181 130 205
Fonds spéciaux	***67 856 000***	***67 856 000***	***67 381 927***	***67 381 927***
GIC	***27 514 650***	***27 514 650***	***28 166 931***	***28 168 931***
Titre2	10 906 848	10 906 848	12 559 129	12 559 129
Hors titre 2	16 607 802	16 607 802	15 607 802	15 607 802
Total action 2	**350 000 399**	**345 403 904**	**352 009 374**	**353 733 321**

Sources : PLF 2017 et 2018

Cette action expose 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)[1].

Vos rapporteurs regrettent toutefois que, dans le Projet annuel de performances annexé au projet de loi de finances, les crédits et les effectifs de l'ANSSI au sein de ceux de l'action 02 ne soient pas présentés de façon plus apparente. Service à compétence national, l'agence pourrait faire l'objet du même traitement que le GIC, d'autant que ses effectifs et les crédits dépensés sont nettement supérieurs, et bénéficier d'une ligne dans la ventilation par destination et titre (p. 32) et dans la ventilation des emplois (p. 36) de la justification au premier euro.

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) et les fonds spéciaux.

Enfin, il permet d'appréhender 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.

[1] *Dans le prolongement des travaux passés de votre commission « 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

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 INTERMINISTÉRIEL DE PRÉVENTION ET 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** et **coordination du renseignement**.

La persistance de la menace terroriste sur le territoire national depuis 2015 a entrainé une intensification de son activité. Le SGDSN est sollicité pour élaborer des réponses en termes 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. Il 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.

Le Secrétaire général assure le secrétariat de ce conseil. **Si en 2015, le CDSN a été réuni à 10 reprises, en 2016, il a tenu 32 réunions et en 2017, de janvier à octobre, a été convoqué 39 fois. Cette fréquence traduit bien l'évolution du conseil dans la conduite et l'orientation de la lutte contre le terrorisme et l'implication des plus hautes autorités de l'Etat dans la définition des orientations et le choix des modes d'action.**

2. Le suivi des conflits et des crises internationales, anticipation et prospectives

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 des travaux interministériels

d'anticipation et de prévention portant ponctuellement sur des pays susceptibles de connaître une crise ou sur des aspects transversaux, afin d'émettre des recommandations aux autorités politiques.

Le SGDSN anime un **comité interministériel de la prospective,** visant à s'assurer de la cohérence et de la coordination des études de prospective menées par les différents ministères dans le domaine de la sécurité et de la défense ainsi que la mise en œuvre des recommandations émises. Une première cartographie des acteurs a été établie en 2016, qui a justifié, en 2017, un approfondissement afin d'améliorer les synergies. Il a piloté la réduction d'une étude prospective sur l'impact des ruptures technologiques dans un environnement stratégique transformé : « Chocs Futurs »[1].

3. Pilotage des stratégies interministérielles

Le SGDSN est en charge de coordonner la réflexion interministérielle sur 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 afin de proposer des orientations et des moyens d'action permettant de renforcer la sécurité nationale. À cet effet, il réalise une évaluation régulière de la **menace terroriste** servant à la réévaluation de la posture VIGIPIRATE.

Il coordonne également les travaux du groupe interministériel sur la **dissémination des armements conventionnels.**

Depuis plusieurs années, **le SGDSN suit la mise en œuvre d'une « *Stratégie Sahel* »,** dont l'objectif est de stabiliser cette région stratégique. Cette stratégie a été actualisée au printemps 2016 en accentuant cette approche globale. Les réunions interministérielles visent à élaborer puis faire le bilan de plans d'action annuels et permettent ainsi aux administrations d'avancer simultanément sur les trois piliers de l'approche globale : l'intervention militaire, le renforcement des capacités de souveraineté et de gouvernance des pays de la zone, l'aide au développement[2]. La nomination d'un envoyé spécial du Président de la République conforte ce travail de coordination. Cette évolution concrétise les propositions du rapport de votre commission sur les interventions extérieures de la France[3], qui a souhaité un renforcement du rôle du SGDSN dans le pilotage de ces stratégies régionales.

---

[1] *Publié au printemps 2017 : http://www.sgdsn.gouv.fr/uploads/2017/04/sgdsn-document-prospectives-v5-bd.pdf*

[2] *Le projet « Alliance pour le Sahel » de l'Agence française de développement (AFD) s'inscrit pleinement dans cette stratégie*

[3] *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*

Le concept d'approche globale est d'ailleurs mis en valeur dans la Revue stratégique de défense et de sécurité nationale d'octobre 2017[1]. Il serait souhaitable de reproduire ce dispositif sur les autres théâtres sur lesquels la France est engagée militairement, à commencer par le Levant. **Vos rapporteurs recommandent d'expertiser cette proposition.**

4. La lutte contre la prolifération

Le SGDSN coordonne les études en matière de **lutte contre la prolifération** des armes de destruction massive et de leurs vecteurs et en produit des documents de synthèse sur les dossiers d'actualité, notamment ceux portant sur **l'Iran, la Syrie ou la Corée du Nord.**

Il assure le secrétariat de diverses instances en charge de **coordonner les évaluations et les moyens de réduire les menaces chimique et biologique**[2] ainsi que **la coordination nationale de la PSI (*Proliferation Security Initiative*),** opération internationale de lutte contre la prolifération des armes de destruction massive ou de leurs composants, au moyen d'échange d'informations et de réalisation d'interceptions des cargaisons.

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 700 ZRR ont été créées.

6. La sécurité des programmes spatiaux européens et contrôle des images spatiales

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*). S'agissant du programme *GALILEO,* il traite les questions liées à la sécurité et au service public réglementé. Il assure, pour la France, la fonction d'Autorité responsable.

Le SGDSN pilote la commission interministérielle des données d'origine spatiale (CIDOS), qui assure le contrôle de diffusion des images spatiales par

---

[1] *http://www.defense.gouv.fr/dgris/la-dgris/evenements/revue-strategique-de-defense-et-de-securite-nationale-2017 § 178 à 180 et 267*

[2] *Avis de la commission des affaires étrangères, de la défense et des forces armées du Sénat n° 142 Tome IX (2016-2017) par MM., Bockel et Masseret, p. 16*

les opérateurs industriels. Les travaux réalisés en 2016-2017 ont permis de mettre à jour la liste des restrictions, qui sera soumise à la validation de la commission.

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

L'**exportation de matériels de guerre** hors de l'Union européenne est soumise à l'obtention d'une **licence**, délivrée par décision du Premier ministre ou, par délégation, du Secrétaire général de la défense et de la sécurité nationale, après avis de la commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG)[1].

Sur la période d'août 2016 à août 2017, la CIEEMG a examiné près de 7 000 dossiers (6 381 en 2015/2016). 95 % des demandes ont fait l'objet d'un traitement en procédure « continue »[2] avec avis favorable, le reliquat est examiné en session plénière.

Le SGDSN conduit les travaux de révision des « directives de haut niveau », qui servent de cadre méthodologique aux décisions. Il a également participé à différents travaux interministériels d'adaptation de la réglementation en matière de contrôle d'armements[3] ou de mise en conformité de celle-ci par rapport à nos engagements internationaux (actualisation de la « liste des matériels de guerre et matériels assimilés »[4]).

En matière de réglementation européenne, il 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).

Il participe activement aux travaux internationaux sur les matériels de guerre et anime le sous-comité de l'accord-cadre « Lettre d'intention »[5], chargé notamment de la simplification des procédures applicables aux transferts entre les six pays membres.

Il préside la commission dite « de l'article 90 »[6]

En 2016, sept opérations sur huit présentées ont fait l'objet d'un avis favorable pour l'octroi d'une avance remboursable pour un montant total de 28 M€. Actuellement, 70 programmes sont en cours d'exécution pour 40 entreprises pour un volume d'encours de plus de 94,4 M€ au 31 décembre 2016. Compte tenu de son caractère autofinancé, le

---

[1] *Loi n° 2011-702 du 22 juin 2011*

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

[3] *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*

[4] *Arrêté de classement du 1er août 2017 modifiant l'arrêté du 27 juin 2012.*

[5] *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).*

[6] *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.*

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[1] et apporte son expertise à la commission interministérielle des biens à double usage (CIBDU) pour l'instruction des dossiers sensibles.

II. LE SGDSN, ACTEUR DE LA POLITIQUE 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. Les réponses que les pouvoirs publics doivent y apporter font l'objet de la stratégie de sécurité nationale.

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[2], qui couvre l'ensemble des travaux destinés à préparer les actions à conduire en situation de crise.

Le nouveau dispositif 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. La rénovation des plans de protection de la « famille pirate » dont le plan VIGIPIRATE de lutte contre le terrorisme

Le plan Vigipirate rénové [3] est entré en vigueur le 1er décembre 2016. Il repose sur un système de niveaux[4] plus cohérent et mieux adapté à la

---

[1] *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.*

[2] 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.*

[3] http://www.sgdsn.gouv.fr/uploads/2017/01/plan-vigipirate-gp-bd.pdf

[4] *Le dispositif comprend désormais trois niveaux : **vigilance** qui correspond à la posture permanente de sécurité et à la mise en œuvre des 100 mesures du socle, toujours actives, **« sécurité renforcée-risque attentat »** des mesures additionnelles (au nombre de 216) peuvent être activées, « **urgence attentat** » déclenché en cas de menace imminente ou suite à un attentat, il est limité à la durée*

menace, la mise en œuvre de nouvelles mesures renforçant l'action gouvernementale dans la lutte contre le terrorisme[1] et le développement d'une culture globale de la sécurité[2].

Par ailleurs, après la validation du plan NRBC en décembre 2016, le plan Piranet en cas d'atteinte majeure à la continuité des systèmes d'information liés aux activités vitales de la Nation et PirateMer de réaction à un acte de piraterie, de brigandage ou de terrorisme en mer ont été testés au cours d'exercices majeurs, approuvés et diffusés en juillet 2017. La révision du plan MétroPirate de réaction à un acte de terrorisme dans les transports collectifs en agglomération a été engagée en 2017. Ces plans sont éprouvés et évalués au cours de grands exercices nationaux. En 2018, ce sera le cas de MetroPirate et de Piratair.

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. Les travaux du CGI se sont accélérés en 2016. Dans le cadre de la montée en puissance du volet NRBC, le SGDSN a apporté un soutien financier substantiel, notamment pour l'acquisition d'équipements pour un montant de 4,4 M€[3]. Cet effort financier a été prolongé en 2017 et 2018[4] à moindre hauteur.

S'agissant de la dimension internationale de la gestion des crises majeures, le SGDSN soutient le Secrétariat général des affaires européennes pour la mise en œuvre de la stratégie de sécurité intérieure de l'UE, il

---

d'activation de la cellule de crise et comporte des mesures exceptionnelles de protection à leur plus haute niveau d'intensité.

[1] Mise en alerte de capacités de lutte contre la menace NRBC, planification et organisation des contrôles aux frontières, mise en œuvre de mesures de police administrative

[2] Publication de guides de bonnes pratiques : http://www.sgdsn.gouv.fr/publications/

[3] Ces crédits ont été alloués au ministère de l'intérieur pour l'acquisition de tenues de protection au profit de la police et de la gendarmerie, de lots pour les points de regroupement des victimes et d'unités mobiles de décontamination pour la sécurité civile.

[4] Au profit des ministères des solidarités et de la santé d'une part, de l'intérieur, d'autre part.

poursuit, en lien avec le coordonnateur national du renseignement et de la lutte contre le terrorisme et les ministères concernés, des actions de coopération en particulier avec le Royaume-Uni, les États-Unis d'Amérique et l'Allemagne. Enfin, il a participé à des actions de coopération avec le Sénégal dans le cadre de la gestion de crise et des discussions sont en cours avec plusieurs États dans le cadre de la mise en œuvre de la force sur les navires à passagers.

Le travail de révision de la circulaire du 2 janvier 2012 relative à l'organisation gouvernementale pour la gestion des crises majeures se poursuit au sein du SGDSN, notamment pour prendre en compte les enseignements tirés de la gestion de crise du cyclone IRMA qui a traversé les Petites Antilles début septembre 2017.

Le SGDSN a poursuivi, en 2017, les travaux qui ont permis d'adopter une feuille de route interministérielle autour de huit actions couvrant les questions d'organisation, de formation et de construction des outils du futur réseau interministériel de logisticiens. La *cellule de coordination interministérielle en logistique* (CCIL) a été créée. Cette dimension a été au cœur de la gestion de crise du cyclone IRMA début septembre 2017.

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

Le secteur français des industries de sécurité représente un chiffre d'affaires de 30 Mds € (dont 21 pour le secteur industriel) et 300 000 emplois (dont 125 000 dans l'industrie) ; il réalise 50% de son chiffre d'affaires à l'exportation.

Le comité de la filière industrielle de sécurité (CoFIS)[1], dont le SGDSN assure le secrétariat, promeut la compétitivité de ce secteur. Il s'articule avec les plans la stratégie nationale de recherche et de la « Nouvelle France Industrielle » notamment son volet « confiance numérique et cybersécurité ». Deux actions importantes sont lancées à l'automne 2017 : la mise en place d'un observatoire de la filière et la rédaction d'un document de politique industrielle mentionnant les principaux objectifs de la filière industrielles des technologies de sécurité à l'horizon 2025.

Les activités du CoFIS

Le SGDSN continuera en 2018 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). Dans le PLF 2017, 2,2 M€ en AE et 1,9 M€ en CP étaient destinés à ces actions, dans le PLF 2018 les montants prévus sont de 1,3 M€ en AE et 1,5 M€ en CP

[1] *installé par le Premier ministre le 23 octobre 2013*

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 et PLF 2017 et 2018

La filière, à travers le CoFIS, s'est mobilisée pour proposer plusieurs projets fédérateurs au PIA2 (PIAVE). Cependant, le financement et les incitations proposés actuellement par le *commissariat général à l'investissement* (CGI) ne permettent pas aux industriels de s'engager dans ces travaux et les dossiers sont toujours en cours d'instruction[1]. La filière confirme le niveau d'investissement national nécessaire dans les années à venir, formalisé par ailleurs dans son document de politique industrielle, et souhaite que la sécurité soit au bon niveau de financement et d'incitation dans le PIA3.

Vos rapporteurs partagent ces préoccupations. 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 reste nécessaire.

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

a) Les capacités liées à la protection du territoire national

Suite à un important travail interministériel conduit par le SGDSN, le Premier ministre a adopté le 14 novembre 2017 la **nouvelle instruction interministérielle relative à l'engagement des armées sur le territoire national lorsqu'elles interviennent sur réquisition de l'autorité civile.**

b) La sûreté des transports

Cible privilégiée de la menace terroriste, les secteurs des transports font l'objet de dispositifs nationaux destinés à renforcer la sécurité. **Le SGDSN a coordonné les travaux interministériels qui ont permis la constitution d'un plan comprenant plus d'une cinquantaine d'actions** qui s'articulent autour de cinq axes : connaissance de la menace, protection des réseaux et infrastructures, efficacité du contrôle des passagers, amélioration du contrôle et de l'accompagnement des opérateurs, développement des patrouilles armées dans les transports.

Un nouveau rapport d'étape a été transmis au Premier ministre en juillet 2017 pour optimiser la coordination et le pilotage politique des enjeux de **sûreté des transports terrestres** à l'instar des dispositifs existants pour le transport aérien et le domaine maritime.

---

[1] *On peut noter deux démonstrateurs d'envergure relatifs à la ville sécurisée, et l'identité numérique qui ont fédéré des grands groupes et des PME. Ces projets ont été labellisé par le COFIS.*

Dans le domaine de la **sûreté aérienne et aéroportuaire**, plusieurs programmes interministériels d'envergure sont menés pour prendre en compte les nouvelles formes de menaces (engins explosifs improvisés, missiles sol-air portables drones …). Les aéroports français en zone de sureté à accès réglementé (ZSAR) bénéficient d'un niveau de protection satisfaisant, cependant les attaques terroristes récentes (Bruxelles, Istanbul) ont révélés les vulnérabilités des zones publiques qui font aujourd'hui l'objet d'un programme prioritaire de renforcements de la sécurité. Enfin, pour prendre en compte les risques de radicalisation rapide, un dispositif de criblage régulier des titulaires d'habilitation autorisant l'accès en ZSAR est mis en œuvre depuis 2017 en attente du déploiement à la fin du premier semestre 2018 d'un système automatisé.

Dans le domaine de la **sûreté maritime et portuaire**, le SGDSN procède à la révision de la doctrine nationale de sûreté. Il pilote en liaison avec le secrétariat général de la mer les échanges avec les États côtiers de destination des navires à passagers sous pavillon français. Avec la Grande-Bretagne, un arrangement administratif sur le déploiement de militaires à bord a été conclu en décembre 2016 auquel devrait se substituer en 2018 un accord intergouvernemental franco-britannique relatif à la sureté maritime et portuaire en Manche et en mer du Nord.

c) 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) par la révision des directives nationales de sécurité (DNS). 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 ANSSI.

Sur la base du mandat reçu du Premier ministre[1] et du bilan complet transmis le 3 mai 2016, le SGDSN conduit des travaux interministériels visant à renforcer la sécurité des sites classés « SEVESO ». 80 sites classés[2] ont été identifiés comme susceptibles d'être désignés PIV (points d'importance vitale) en plus des 60 existants et font l'objet de procédures de désignations. Une offre de solutions de sécurité est proposée aux exploitants en concertation avec les fédérations industrielles concernées et le financement d'un projet de suivi et de traçabilité des personnes intervenant sur un site sensible devrait être engagé dans le cadre du programme d'investissement d'avenir.

[1] *à la suite des événements survenus en 2015 à Saint-Quentin-Fallavier et à Berre-l'Etang*
[2] *Parmi les quelque 1 200 sites classés « SEVESO ».*

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[1].

d) 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 2017 de nombreux projets, 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 fait partie des actions menées[2].

Sur la base du retour d'expérience de l'épisode de crues en Ile-de-France en juin 2016 et de l'exercice « Crue de Seine 2016 », le SGDSN a révisé le plan de continuité du travail gouvernemental en cas de crue majeure à Paris et lancé l'élaboration d'un plan d'action pour le renforcement de la logistique ministérielle en cas de crise, incluant une réflexion sur les capacités d'évacuation massive de population.

En 2017, trois exercices ont été organisés sur les questions de contre-terrorisme maritime, de sécurité des transports et de danger NRBC.

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

Une révision de l'instruction générale interministérielle n° 1300 du 30 novembre 2011 sur la protection du secret de la défense nationale 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 en cours de validation, pourrait entrer en vigueur courant 2018.

Votre commission avait souhaité qu'un effort de formation continue soit engagé en direction des administrations et des entreprises des secteurs sensibles. La formation et la sensibilisation à la protection du secret ont fait l'objet d'une réflexion approfondie pour améliorer le dispositif global. Un renforcement des actions d'information est explicitement demandé aux acteurs de la protection du secret dans le projet de texte. Le SGDSN développe des outils d'accompagnement et un partenariat avec un institut de formation est à l'étude.

---

[1] *Avis de la commission des affaires étrangères, de la défense et des forces armées du Sénat n° 142 Tome IX (2016-2017) par MM., Bockel et Masseret, p. 26*

[2] *Cette politique a pour ambition de conseiller les responsables de sites accueillant du public et la population afin d'accroître leur niveau de vigilance et de les impliquer dans l'acquisition de bonnes réactions. Cet effort s'est traduit par l'élaboration et la large diffusion d'un document d'ensemble. Des fiches pratiques accompagnent dorénavant les postures Vigipirate à l'attention des opérateurs, des collectivités territoriales, voire du grand public.*

Vos rapporteurs saluent cet effort. Ils proposent également qu'une formation initiale soit donnée dans les écoles d'ingénieurs et dans les écoles de formation des futurs cadres des entreprises (écoles de commerce et de gestion) et des administrations (ENA, IRA…).

Par ailleurs, les négociations en vue de la signature d'accords généraux de sécurité (AGS) se poursuivent. A ce jour 39 accords ont été conclus.

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

Le SGDSN propose de mettre en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information[1]. Il dispose à cette fin de l'ANSSI[2]. Le positionnement de l'Agence auprès du SGDSN a permis de faire valoir les enjeux au plus haut niveau de l'État. Il a, en revanche, pour inconvénient, d'inscrire l'ANSSI dans un circuit de décisions administratives et budgétaires contraignant.

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

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

- « 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 2016 de l'ANSSI donne une vision détaillée des missions actuelles et à court terme[3].

A. UNE MENACE QUI NE CESSE DE S'ACCROÎTRE EN INTENSITÉ ET EN SOPHISTICATION

L'ANSSI constate une sophistication croissante des attaques informatiques, notamment de celles menées par des acteurs étatiques ou paraétatiques à des fins d'espionnage, et le développement des actions d' « hacktivisme » et de déstabilisation à grande échelle, souvent via les réseaux sociaux, mettant en œuvre des modes d'action tels le recueil et la divulgation massive de données sensibles.

---

[1] *Article R 312-3 du code de la défense*

[2] *Service à compétence nationale, dont les missions sont définies par le décret n° 2009-834 du 7 juillet 2009 modifié.*

[3] https://www.ssi.gouv.fr/uploads/2017/06/dossier_presse_rapport_activite_2016_anssi.pdf

Il existe un continuum entre cybercriminalité et sécurité nationale. Ainsi, à grande échelle, l'utilisation d'outils d'extorsion de fonds comme les « rançongiciels », peut peser gravement sur la continuité d'activités vitales pour la Nation, paralysant, par exemple, l'activité d'entreprises d'importance stratégique.

La commercialisation de capacités offensives comme la prolifération d'outils, gratuits ou bon marché, et de compétences facilitant le lancement des attaques, constituent des phénomènes émergents et inquiétants.

Le domaine cybernétique est reconnu comme un nouvel espace de conflictualité dans les doctrines militaires, ce qui se traduit par la création de structures de forces dans la plupart des grandes puissances, France incluse[1].

Enfin la dépendance croissante aux systèmes numériques couplée à une insuffisante prise en compte des enjeux de cybersécurité dans leur architecture et leur développement accroît leur vulnérabilité.

La France est classée désormais au 8e rang mondial des pays où la cybercriminalité est la plus active et au 4ème rang européen

Les données rassemblées par Symantec dans le rapport *Internet Security Threat Report* (ISTR) met en avant les tendances marquantes

Le rapport observe une recrudescence des e-mails contenant des pièces jointes malveillantes par rapport à ceux contenant des liens pointant vers des sites de phishing qui ont reculé. Un mail sur 131 est malveillant dans le monde (1/209 en France) contre 220 en 2015. Ce sont des campagnes de mails malveillants qui ont ciblé la campagne électorale de Mme Clinton aux Etats-Unis. Symantec relève que le cyber espionnage a expérimenté une évolution notable vers des modes d'action plus ouverts, destinés à déstabiliser et à perturber les organisations et les pays ciblés.

Symantec a enregistré une hausse de 36 % du nombre de rançongiciels et en a identifié plus de 100 nouvelles familles dans le monde. Cette activité se révèle toujours lucrative, Le montant des cyber-rançons est passé en un an de 294 à 1 077 $. Ce type d'attaques n'a pas progressé en France sans doute parce que seules 30% des victimes paient les rançons contre 64% aux États-Unis. On notera qu'en mai 2017, l'attaque massive à base de logiciels malveillants « WannaCry ou WannaCrypt » a probablement touché plus de 100 000 systèmes dans près de 100 pays dont le service de santé britannique et de nombreuses entreprises industrielles ou de services qui ont dû interrompre leurs activités

En revanche, la France n'est pas épargnée par les vols d'identifiants. Avec 85,3 millions d'identifiants volés, elle pointe à la 2ème place derrière les États-Unis (791,8).

Les risques liés à l'Internet des Objets se confirment. Le réseau de programmes connectés à Internet Mirai a été utilisé dans la plus grande attaque par déni de service distribuée[2] fin 2016.

[1] http://www.defense.gouv.fr/actualites/articles/cyberdefense-bilan-et-nouveaux-chantiers-annonces-par-le-ministre

[2] *Attaque ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. À l'heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée.*

Au plus fort de l'activité, lorsque Mirai se développait, Symantec enregistrait des attaques toutes les 2 minutes.

Sources :
Symantec https://www.symantec.com/fr/fr/security-center/threat-report

Le Monde informatique – 27 avril 2017 « Ramsomeware, seulement 30% des rançons versées en France contre 64% aux Etats-Unis » Dominique Filippone

Libération 13 mai 2017 Amaelle Guiton « Ce que l'on sait des cyberattaques visant plusieurs pays »

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

Engagée par la loi de programmation militaire (LPM) 2014-2019, prolongée en 2015 par la stratégie nationale pour la sécurité numérique[1], cette démarche sera poursuivie et accentuée dans les suites qui seront données aux recommandations de la revue stratégique de la défense d'octobre 2017[2] et de la revue stratégique de cyberdéfense en cours[3] avec la mise en œuvre d'une **posture permanente de cybersécurité plus robuste**.

L'un des axes retenus dans la stratégie de l'ANSSI pour la période 2016-2020, intitulé « connaissance et anticipation » a pour objectif de renforcer sa capacité à mener des travaux de prospective, 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.

Au cours de l'année 2017, l'ANSSI a participé à de nombreux travaux de prospectives engagés par d'autres administrations ou autorités indépendantes[4].

Elle a organisé, en avril 2017 à l'UNESCO, 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 et de promouvoir la prévention de l'utilisation de capacités cyber offensives par les acteurs non-étatiques.

Pour mener ses missions au niveau stratégique, elle s'est dotée d'une « cellule d'anticipation cyber » rattachée à son directeur général. Dans le cadre de la revue stratégique de cyberdéfense, elle a proposé de mettre en place et d'animer un groupe d'experts en charge d'organiser la veille technologique, d'anticiper les évolutions et de proposer les réponses adaptées.

---

[1] *https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_dossierpresse.pdf*

[2] *Revue stratégique de défense et de sécurité nationale 2017 p.35, 46 & 47, 67,73*

[3] *Annoncée à l'issue du conseil de défense et de sécurité nationale du 19 juillet 2017.*

[4] *Ainsi, l'agence a notamment contribué au rapport thématique « Chocs Futurs », étude prospective à l'horizon 2030 des impacts des transformations et ruptures technologiques sur notre environnement stratégique et de sécurité, réalisé par le SGDSN ; à l'étude menée par l'ARCEP relative aux objets connectés ; au groupe de travail relatif à l'intelligence artificielle animé par la direction interministérielle du numérique et du système d'information de l'Etat et aux travaux lancés par la Caisse des Dépôts dans le cadre du « laboratoire d'innovation » destiné à anticiper les risques induits par la technologie blockchain.*

C. UNE CAPACITÉ D'EXPERTISE DE TRÈS HAUT NIVEAU

L'ANSSI constitue un vivier d'expertise de haut niveau au profit de l'ensemble des services de l'Etat et, à ce titre, apporte son soutien technique à de nombreux projets informatiques sensibles (système *Titres électroniques sécurisés*, système d'information des élections, projet *France Connect*).

Elle conduit des activités de recherche scientifique et technique afin d'assurer le maintien à l'état de l'art des expertises nécessaires à tous les domaines liés au numérique, en lien avec les acteurs publics et privés de l'écosystème. Sept laboratoires thématiques, intégrés à la sous-direction Expertise[1], concentrent l'essentiel des activités de recherche de l'agence[2].

D. LES ACTIONS DE L'ANSSI VERS LES ADMINISTRATIONS

En collaboration avec les administrations compétentes, l'ANSSI instruit et prépare les décisions gouvernementales relatives à la sécurité du numérique et à celle des données sensibles. Elle participe à la construction et à la maintenance des réseaux et terminaux sécurisés de l'Etat.

1. La protection de l'information de souveraineté

L'ANSSI a pour mission la conception et le maintien en condition opérationnelle et de sécurité des systèmes d'information gouvernementaux classifiés de défense interministériels. Depuis 2013, en partenariat étroit avec le Centre de transmission gouvernemental (CTG), elle développe, déploie et assure le support technique des systèmes de communications sécurisés et apporte son soutien à la direction interministérielle du numérique et des systèmes d'information et de communication (DINSIC) pour l'équipement de l'ensemble des cabinets ministériels[3].

2. La lente mise en œuvre de la politique de sécurité des systèmes d'information de l'Etat (PSSIE)

Le Premier ministre a publié, en 2014, une circulaire préparée par l'ANSSI fixant les contours d'une « *Politique de sécurité des systèmes*

---

[1] *La division « scientifique et technique compte 58 agents ,la moitié titulaires d'un titre de docteur.*

[2] *Avis de la commission des affaires étrangères, de la défense et des forces armées du Sénat n° 142 Tome IX (2016-2017) par MM., Bockel et Masseret, p. 35*

[3] *Pour mémoire, l'ANSSI s'est portée fin 2015 acquéreur d'une licence globale libératoire pour l'utilisation, par les services de l'État, d'un ensemble de logiciels de chiffrement qualifiés auprès de la société Prim'X. En 2016 plus de 600 000 postes ont été équipés.*

d'information de l'État » (PSSIE)[1] **et des règles de protection**[2]. Elle constitue un élément de réponse essentiel aux cybermenaces.

La mise en conformité des ministères se poursuit sous le pilotage des services des hauts fonctionnaires de défense et de sécurité. L'ANSSI assure un service interministériel de supervision.

Dans leur avis sur le PLF 2017[3], vos rapporteurs s'inquiétaient de la lenteur de ce processus.

Trois ans après sa publication, la PSSIE a été adoptée par l'ensemble des ministères. **Entre 2016 et 2017, le niveau effectif de conformité**, qui fait l'objet d'un indicateur[4] sous l'objectif 6 du programme 129 « *améliorer la sécurité et la performance des systèmes d'information de l'Etat* », **tarde à atteindre des niveaux en adéquation avec les enjeux portés par les systèmes d'information de l'Etat.** « *Ces retards sont observés pour la plupart du temps au sein des ministères non régaliens. Le comblement de ce retard dans les deux ans doit permettre d'afficher un niveau moyen plus conforme à l'horizon 2020*. »

Les plans d'action engagés par les différents ministères devraient permettre une accélération de leur progression, notamment en matière de gouvernance et de maîtrise des risques. Cependant, **cette politique se heurte à l'insuffisance des moyens organisationnels et budgétaires consacrés à la sécurité dans les ministères pour atteindre une situation satisfaisante.**

En sa qualité d'autorité nationale de sécurité et de défense des systèmes d'information, l'ANSSI porte la capacité nationale de détection des attaques et met en œuvre un service interministériel de supervision qui s'appuie sur des sondes de détection positionnées sur les réseaux des ministères et sur le réseau interministériel de l'Etat (RIE). Ce système a montré son efficacité mais il se heurte à des contraintes techniques et d'organisation qui ne permettent pas toujours à l'ANSSI de déployer des sondes dans des conditions adaptées à la menace, ni de recueillir toutes les informations nécessaires pour assurer une détection optimale.

Cette situation reste insatisfaisante au regard des objectifs de conformité complète à la PSSIE. Pour la deuxième année, vos rapporteurs s'inquiètent de la lenteur du processus. Ils attirent l'attention du Premier ministre sur l'acuité de la menace (cf les attaques en 2017 contre le système de santé britannique) et lui demandent de sensibiliser avec fermeté

---

[1] *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.*

[2] *n° 5725/SG du 17 juillet 2014.*

[3] *Avis de la commission des affaires étrangères, de la défense et des forces armées du Sénat n° 142 Tome IX (2016-2017) par MM., Bockel et Masseret, p. 37 et suiv.*

[4] *Indicateur 6-1 « Niveau de sécurité des systèmes d'information de l'Etat »*
https://www.performance-publique.budget.gouv.fr/sites/performance_publique/files/farandole/ressources/2017/pap/html/DBGPGMOBJINDPGM129.html

l'ensemble des ministres, seuls les ministères de la défense et de l'intérieur ont produit les efforts nécessaires. Ils demandent qu'une évaluation soit conduite par un corps d'inspection en vue d'identifier les difficultés et de proposer un plan d'actions destinées à accélérer la mise en œuvre de ces dispositions par les ministères concernés. Ils souhaitent que soient étudiés rapidement les moyens juridiques et techniques permettant à l'ANSSI de disposer de moyens de contraintes pour imposer ses préconisations aux directions des systèmes d'information des ministères.

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

Le Centre de formation à la sécurité des systèmes d'information (CFSSI) assure la formation des agents de l'État en matière de cybersécurité et propose un important catalogue de stages adaptés à la multiplicité des besoins et des profils. En 2016, 1 699 stagiaires ont participé aux 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 2016, le titre d'expert a été attribué à 21 élèves (8 en 2015).

3. La politique d'investissement de l'ANSSI

L'ANSSI prévoit le développement de programmes de sécurité sur le budget quinquennal pour répondre aux évolutions suivantes :

- la menace (augmentation du nombre d'attaquants et décuplement de leurs capacités) ;
- les technologies (cycles de vie des technologies de plus en plus courts, à l'instar des générations de réseaux mobiles) ;
- les usages (développement des *smartphones* notamment).

Plusieurs programmes doivent ainsi être engagés, parmi lesquels :

- « Chiffrement IP » et « Crypsis NG » : programmes ayant pour objet d'assurer la protection de flux classifiés, véhiculés à travers internet (à mettre en relation avec les besoins du GIC pour la centralisation du renseignement) ;
- « Sondes CD » : programme visant à renforcer la détection des attaques par le déploiement de sondes dans les réseaux, capables d'identifier différentes classes d'attaques ;
- « Mobilité CD » et le développement des réseaux sécurisés : programmes destinés à améliorer la protection des informations classifiées de défense, avec pour objectif premier de garantir la confidentialité, l'intégrité et la résilience des communications de l'administration et de permettre dans certains cas d'échanger avec nos alliés dans le cadre de l'OTAN ou de l'Union Européenne.

Au-delà de ces programmes majeurs, le SGDSN poursuivra le financement du *data center*.

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. En contrepartie de la mise à disposition de structures et de leur exploitation par le ministère de l'intérieur pendant une durée minimale de 15 ans, le SGDSN s'est engagé à participer à la réalisation du centre proportionnellement aux surfaces occupées, soit 75% du coût global des travaux. En phase d'exploitation, le ministère de l'intérieur assurera au profit de l'ANSSI les actions de proximité permettant une exploitation à distance. Les incidences pour les ressources humaines de l'agence seront dès lors limitées.

4. Une capacité centralisée de détection et de réponses aux attaques informatiques

L'ANSSI a mis en place depuis 2010 un Centre opérationnel de la sécurité des systèmes chargé de détecter et d'entraver les attaques visant notamment les systèmes d'information de l'État et des opérateurs d'importance vitale. Sa mission va de l'analyse des menaces et des vulnérabilités à la remédiation post-crise, en passant par la qualification des attaques en cours et la définition des mesures de réponse. Dans ce cadre, l'ANSSI 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. Le rapport annuel de l'ANSSI montre le niveau intense de l'activité du COSSI et son implication dans l'accompagnement de la reprise de contrôle des systèmes d'information[1].

Enfin, il réalise plusieurs dizaines de prestations d'audit au profit de l'administration ainsi que des opérateurs d'importance vitale privés[2].

E. L'ÉLARGISSEMENT DU PÉRIMÈTRE D'ACTION

La LPM 2014-19 et la stratégie numérique du gouvernement de 2015 ont fixé des orientations stratégiques et des priorités complémentaires en matière de protection des systèmes d'information des opérateurs d'importance vitale et d'assistance aux victimes des actes de cyber malveillance. L'ANSSI les accompagne dans la sécurisation de leurs systèmes d'information critiques. Cette sécurisation passe, entre autres, par

[1] *Rapport annuel d'activité de l'ANSSI pour 2016 p.31 et 32* https://www.ssi.gouv.fr/uploads/2016/09/rapport_annuel_anssi_2016.pdf

[2] *L'ANSSI a réalisé en 2016, 59 audits auprès des ministères et des OIV : 60% d'audits à la demande, 28% à l'occasion d'opérations, 10% dans le cadre d'inspections ministérielles et 2% à l'occasion de missions de contrôle.*

l'application d'un corpus de règles de sécurité définies par l'ANSSI et les opérateurs ainsi que par la mise en place d'un dispositif de détection d'incidents et d'attaques.

La directive européenne relative à la sécurité des systèmes d'information, dite NIS, adopté en juillet 2016, qui sera examiné au Sénat d'ici la fin de l'année, conforte ces orientations. La mise en place de la notion d'opérateurs de services essentiels permettra d'englober des entités au-delà des actuels OIV[1].

La revue stratégique de défense présentée le 11 octobre met l'accent sur l'importance des menaces et esquisse de nouvelles orientations stratégiques[2] qui seront précisées par la revue stratégique de cyberdéfense.

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

Pour la réussite des missions auprès des opérateurs d'importance vitale, qui appartiennent au secteur privé (environ 230 organisations), la LPM 2014-2019, par un dispositif réglementaire, a permis d'engager une dynamique permettant d'ici quelques années d'atteindre un niveau acceptable de sécurité de leurs systèmes d'information.

En application de l'article 22 de la loi, neuf arrêtés sectoriels ont été publiés par les ministères compétents en 2016[3], cinq arrêtés ont été publiés en 2017, et deux autres devraient l'être d'ici la fin de l'année[4].

Lors de l'entrée en vigueur des arrêtés les concernant, les OIV sont tenus de mettre en place les 20 règles de sécurité définies par l'ANSSI et de lui déclarer leurs incidents de sécurité. Dans un délai de trois mois, ils doivent également avoir identifié et déclaré leurs systèmes d'information d'importance vitale. L'ANSSI a commencé en 2017 à apporter aux OIV un accompagnement technique et à recueillir leurs premières déclarations.

La mise en œuvre de ce nouveau dispositif s'appuie largement sur l'industrie de la cybersécurité, *via* la qualification par l'ANSSI de prestataires de services de confiance (détection, audit, réponse aux incidents…) et de produits de sécurité (sondes de détection). Le décret n° 2015-350 relatif à la

---

[1] *Voir supra p.33 et suiv.*

[2] *Revue stratégique de défense et de sécurité nationale 2017 p.88 à 91, 133 à 136, 252 et 260*

[3] *Les arrêtés relatifs aux secteurs d'activité* « produits de santé », « gestion de l'eau » *et* « alimentation » *sont entrés en vigueur au 1er juillet 2016, et ceux relatifs aux secteurs* « transports terrestres », « transports maritime et fluvial », « transport aérien », « approvisionnement en énergie électrique », « approvisionnement en gaz naturel », « approvisionnement en hydrocarbures pétroliers » *au 1er octobre 2016.*

[4] *En 2017, sont entrés en vigueur les arrêtés relatifs aux secteurs* « audiovisuel et information », « communications électroniques et Internet », « finances » *et* « industrie » *le 1er janvier, et au secteur* « nucléaire » le 1er avril. *La parution des derniers arrêtés couvrant les secteurs* « espace » *et* « activités industrielles de l'armement » *devrait intervenir avant la fin de l'année 2017*.

qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale précise les conditions de délivrance de ces qualifications.

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.**

Vos rapporteurs regrettent que la sécurité des systèmes d'information des opérateurs d'importance vitale encadrée par les articles L. 1332-6-1 et 6-7 du code de la défense ne constitue pas un objectif du programme 129. L'ANSSI produit pour son usage interne, un indicateur des progrès réalisés dans la protection des systèmes d'information des OIV. **Ils réitèrent leur demande, formulée dans l'avis sur le projet de loi de finances pour 2017, qu'elle fasse l'objet d'un objectif du PAP et d'un indicateur de performance permettant de 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, un tableau de bord synthétique sur les infractions constatées et les mesures de remédiation réalisées.**

2. La protection des réseaux

La sécurisation des réseaux de télécommunications est un enjeu clé. L'agence joue un rôle central dans le contrôle réglementaire instauré en application de l'article 226-3 du code pénal qui soumet à autorisation la commercialisation et la détention d'équipements susceptibles de porter atteinte à la confidentialité des communications électroniques[2].

Sous son égide, l'Observatoire de la résilience de l'Internet français contribue à améliorer la compréhension collective de ce réseau par l'étude des technologies susceptibles d'entraver son bon fonctionnement.

Dans le sillage des recommandations déjà élaborées sur la sécurité des réseaux de téléphonie mobile, l'ANSSI a transmis en 2016 aux opérateurs de communications électroniques de nouvelles recommandations[3].

---

[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.*

[2] *Ce régime de contrôle a été étendu par un arrêté du 11 août 2016 qui a permis de soumettre de nouveaux équipements au contrôle R226, notamment les «stations de bases» de réseau mobile, susceptibles, selon leurs caractéristiques, de permettre des interception du trafic. Ces nouvelles mesures sont assorties d'un délai d'application de cinq ans, pour permettre aux opérateurs d'intégrer ces exigences dans leur calendrier de déploiement à l'horizon 2020 des réseaux de 5ème génération.*

[3] *Les sujets abordés: les réseaux de téléphonie mobile 4G et les services DNS (*Domain name system*) utilisés par les équipements de cœur de réseau mobile afin d'améliorer la sécurité de ces réseaux et de protéger les abonnés lors des différents cas d'itinérance.*

Parallèlement, ses équipes techniques ont poursuivi les actions destinées à mieux appréhender les enjeux de sécurité liés à la virtualisation croissante des fonctions de cœur de réseau et approfondi d'autres travaux sur la sécurisation des moyens d'administration des réseaux ainsi que sur la sécurisation des messageries grand public.

3. L'entrainement à la gestion des crises

Autorité nationale de cyberdéfense, l'ANSSI est responsable de l'entrainement des autorités publiques et des OIV à la mise en œuvre des mesures destinées à répondre aux crises majeures affectant leurs systèmes d'information. Elle est donc fortement impliquée dans l'organisation et le jeu d'exercices, à la fois au niveau national et au niveau international.

En France, un exercice majeur de gestion de crise d'origine cybernétique a permis, fin 2016, de tester le plan « Piranet » et de le diffuser fin juillet 2017. En outre, depuis 2015, chaque exercice majeur planifié par le SGDSN inclut un volet cybernétique, pour familiariser les acteurs de la gestion de crise avec cette problématique qui accompagne et complique le règlement des crises. L'ANSSI est également partie prenante dans la mise en œuvre de la réserve de cyberdéfense et contribue à la définition de son concept d'emploi. Elle est impliquée dans la planification et le jeu des exercices DEFNET, organisés sous la responsabilité du ministère des armées.

L'agence participe à la série Cyber Europe de UE ainsi qu'aux exercices de l'OTAN Cyber Coalition, *Locked Shield* et CMX (quand ils comportent un volet cybernétique).

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

L'ANSSI est un acteur majeur de la promotion d'une culture de cybersécurité. Dans le cadre de la stratégie du numérique d'octobre 2015, elle a préparé la mise en place depuis le 17 octobre 2017 d'une plateforme numérique destinée à mettre en relation des victimes d'actes de cyber malveillance avec des prestataires privés susceptibles de les accompagner dans le traitement des incidents de sécurité informatique[1]. Cette plateforme sera également un observatoire du risque numérique dont les données permettront d'évaluer l'exposition à la cybermalveillance des entreprises, des collectivités territoriales et des particuliers.

L'ANSSI finance le dispositif constitué sous forme de groupement d'intérêt public (GIP)[2] à hauteur de 0,9 M€. Sa participation devrait décroitre au fur et à mesure de l'association de nouveaux partenaires. La plateforme emploie 8 personnes.

---

[1] https://www.cybermalveillance.gouv.fr/ .

[2] *Dont le directeur général de l'ANSSI assure la présidence, ce qui permet une association avec les administrations concernées, les consommateurs, les prestataires de sécurité informatique, les opérateurs de communications électroniques et les éditeurs.*

En parallèle, l'ANSSI a développé une politique active de sensibilisation et de communication[1].

Elle met en place des relais dans des 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. L'agence déploie un réseau de correspondants afin de développer ses actions d'information et de conseil. En 2016, elle a conduit 500 interventions en région. Toutes les régions métropolitaines devraient être dotées d'un référent d'ici fin 2017.

Une fois consolidée, la coopération avec les services déconcentrés de l'État est complétée par un rapprochement avec les collectivités territoriales, et tout particulièrement les régions, compte tenu de leurs compétences en matière de développement économique. Les actions visent notamment à une meilleure intégration des questions liées à la sécurité du numérique, en amont des grands programmes de développement, de formation et de recherche portés par les régions.

La proximité des référents a permis d'établir des liens plus directs avec les opérateurs d'importance vitale implantés en régions et de leur fournir une assistance adaptée. Le volume des sollicitations reçues par les référents montre également une attente très forte de la part des collectivités territoriales et des acteurs privés.

5. La mise en place de l'identité numérique

Dans le domaine juridique, l'ANSSI a piloté la rédaction de plusieurs textes d'application de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique[2] et apporté son soutien technique à la DINSIC dans le cadre des projet *France Connect* qui offre une solution d'identités électroniques permettant d'accéder aux services publics numériques et facilitant l'échange de données entre administrations.

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

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 constituent une réponse à la permanence, à l'intensité et à la complexité de la menace. Dans cette perspective, l'ANSSI mène des actions de politique industrielle, en étroite concertation avec d'autres

---

[1] *Elle a publié plus d'une vingtaine de supports de sensibilisation dont un guide de l'hygiène informatique recensant 42 mesures de bases. Elle est présente sur Internet, sur les réseaux sociaux, développe ses relations presse et participe à de nombreux colloques et évènements spécialisés*

[2] https://www.economie.gouv.fr/republique-numerique

administrations, notamment la direction générale des entreprises et la direction générale de l'armement avec 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.

Ces actions s'inscrivent dans le plan d'action « cybersécurité » de la solution « Confiance Numérique » de la nouvelle France Industrielle. Ce plan s'organise autour de quatre axes : l'accroissement de la demande en solutions de cybersécurité de confiance, le développement d'offres de confiance, l'organisation de la conquête des marchés à l'étranger et, enfin, le renforcement des entreprises nationales du domaine cyber sécurité.

Cette initiative a entraîné le lancement de nombreuses actions concrètes :

+ + l'orientation des appels à projets du programme d'investissements d'avenir (PIA) : l'ANSSI assure le pilotage de 7 projets dans les domaines de la détection d'attaques informatiques, de la sécurité des réseaux industriels et de la téléphonie sécurisée, lesquels font l'objet d'un soutien financier global de l'ordre de 18 M€. 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[1] ;

+ un volet de labellisation qui, outre les labels délivrés par l'ANSSI[2], intègre un label « France Cybersecurity » dont la gestion est assurée par la filière industrielle elle-même[3];

+ un volet de formation, avec le recensement des besoins qualitatifs et quantitatifs en personnels formés des entreprises nationales du secteur, des actions en faveur de l'insertion de la cybersécurité dans les formations informatiques supérieures[4] et de labellisation des formations spécialisées en sécurité informatique[5] dans le double objectif de valoriser ces

---

[1] *Plusieurs projets ont été soutenus en 2017 en faveur de TPE/PME en vue de la certification et la qualification de solutions de cybersécurité. 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 qu'elle pourrait jouer pour mettre en relation ces acteurs avec des entreprises innovantes.*

[2] *Voir infra p.50*

[3] *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 82 solutions nationales et il est régulièrement mis en avant, notamment dans des démarches de promotion à l'export.*

[4] *Le projet CyberEdu promeut l'intégration de la sécurité numérique dans les formations supérieures en informatique non spécialisées en SSI par la fourniture de contenus pédagogiques remis aux enseignants S'ajoute à cela l'organisation par le CFSSI de colloques d'accompagnement des enseignants autour des méthodes d'intégration de la sécurité dans les formations. Elle a publié, en mai et septembre 2017 un premier module de sensibilisation et de formation en ligne (MOOC) « SecNumacadémie » qui vise l'ensemble des utilisateurs du numérique en milieu professionnel.*

[5] *En juin 2017 », 30 formations de niveau master, licence ou licence professionnelle avaient reçu ce label « SecNumedu » lancé en janvier 2017, ce qui représente plus de 800 élèves par an. L'ANSSI estime que 60 formations françaises pourraient être labellisées à terme. Des travaux sont actuellement en cours pour proposer ce label à des formations continues. 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. Ces travaux se*

formations et de faciliter l'identification, par les employeurs ou les étudiants des parcours de formation pertinents ;

+ un volet réglementaire, comportant 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 traduit par l'établissement d'une convention entre l'ANSSI et l'union des groupements d'achats publics (UGAP). L'agence peut également procéder à l'acquisition de licence globale libératoire de logiciels de chiffrement qualifiés[1];

+ un volet d'exportation[2] ;

+ la mise en place d'une plateforme d'échanges entre pouvoirs publics et acteurs industriels, permettant la définition d'une vision partagée des principaux facteurs de développement industriel et le lancement d'actions concrètes. Elle a permis de coordonner la participation et l'action des acteurs français au moment de la création du partenariat public-privé sur la cybersécurité établi en juillet 2016 par la Commission européenne[3].

G. LES RELATIONS INTERNATIONALES

En lien avec les ministères compétents, l'ANSSI assure la représentation de la France dans les organisations internationales, le suivi des négociations en matière de sécurité numérique et l'établissement de partenariats notamment opérationnels avec d'autres pays.

a) La préparation des positions françaises au sein de l'Union européenne

Les institutions européennes considèrent le numérique comme un champ d'action nouveau dans lequel elles disposent d'un pouvoir normatif. L'agence doit ainsi y renforcer son influence afin que les orientations soient conformes à nos intérêts fondamentaux de la France.

La France ayant été l'un des premiers pays européens à mettre en place une approche ambitieuse en cybersécurité, notamment via son choix d'utiliser la réglementation pour protéger les opérateurs d'importance vitale. Ce modèle interministériel, séparant institutionnellement les rôles d'attaque et de défense, a trouvé un écho auprès d'une majorité d'États membres et des autorités européennes.

La France joue également un rôle moteur dans la définition des orientations stratégiques de l'UE. Elle a annoncé officiellement, dans sa

---

sont poursuivis avec la mise en place, par l'ANSSI et en collaboration avec des représentants des organismes de formation et de l'industrie, d'un schéma de labellisation de formations supérieures en sécurité numérique

[1] Voir supra p.24

[2] 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.

[3] A ce titre l'ANSSI a organisé et animé une coordination nationale des acteurs impliqués dans ces travaux visant notamment à définir le cadre d'une certification de sécurité, ainsi que pour les thématiques de recherche et développement européennes dans le domaine de la cybersécurité.

Stratégie nationale pour la sécurité du numérique, son engagement en faveur de l'autonomie stratégique européenne, reposant sur trois piliers : capacitaire, industrielle et technologique et de décision.

(1) La directive sur la sécurité des réseaux et des systèmes d'information dite «directive NIS» (*Network and Information Security*).

L'enjeu de la directive adoptée, le 6 juillet 2016 est d'assurer un niveau élevé et commun de sécurité dans l'UE.

La directive prévoit :
+ le renforcement des capacités nationales de cyber sécurité grâce au positionnement de la cyber sécurité comme un enjeu stratégique majeur pour le marché européen du numérique ;
+ l'établissement d'un cadre de coopération volontaire entre États membres via un groupe de coopération et un réseau européen des CSIRT (*Computer Security Incident Response Team*) afin de renforcer la cyberrésilience ;
+ le renforcement par chaque État de la cybersécurité d'opérateurs de services essentiels ;
+ l'instauration de règles européennes communes à l'intention des prestataires de services numériques dans le but d'encadrer et de réguler la sécurité du numérique.

Les Etats membres auront jusqu'au 9 mai 2018 pour la transposer dans leur droit national. Le texte a été présenté au conseil des ministres le 22 novembre 2017[1]. Le projet de loi sera examiné au Sénat d'ici la fin de l'année.

(2) Un partenariat public-privé dédié à la cyber sécurité (cPPP)

L'objectif de ce nouveau dispositif signé par la Commission, le 5 juillet 2016, est de générer 1,8 Md€ d'investissements via l'effet de levier des 450 M€ provenant des fonds alloués au programme pour la recherche et l'innovation afin d'améliorer la résilience de l'Europe et de renforcer la compétitivité des entreprises européennes du secteur de la sécurité numérique. On estime que les acteurs du marché de la cybersécurité devraient, eux, investir trois fois plus.

(3) La présentation par la Commission européenne d'un « paquet sécurité »

Ce paquet constitue la feuille de route de l'exécutif européen, en matière de sécurité du numérique, jusqu'à la fin de son mandat, en 2019. Il est composé de plusieurs textes de nature distincte[2] notamment une proposition de règlement européen qui regroupe au sein d'un même texte un projet de nouveau mandat pour l'agence européenne de sécurité des réseaux et de l'information (ENISA) et la création d'un cadre européen de certification de sécurité.

---

[1] *http://www.senat.fr/leg/pjl17-105.html*

[2] *Une communication chapeau sur la résilience, la dissuasion et la défense pour la cybersécurité de l'Union européenne listant les actions prioritaires de l'Union européenne pour les prochaines années ; une recommandation proposant un cadre européen de réponse aux crises cyber ; et une communication précisant certaines modalités de mise en œuvre de la directive NIS, adoptée en juillet 2016.*

Ces initiatives européennes doivent faire l'objet d'une attention vigilante, dans un domaine où la souveraineté des Etats est en jeu, notamment lorsqu'il s'agit de la réponse opérationnelle aux cyberattaques ou de la certification aux plus hauts niveaux de sécurité.

Dans sa formulation actuelle, la proposition d'un cadre européen de certification de sécurité ne satisfait pas pleinement l'objectif de renforcement de la cybersécurité de l'UE, soulève de sérieuses préoccupations dans la mesure où il ne tire pas suffisamment parti de l'expertise comme des capacités d'évaluation existant au sein des Etats membres et de leur coopération, lesquels ont fait preuve de leur efficacité, et ne permet pas de construire un cadre susceptible d'évoluer de façon agile à l'état de l'art et aux développements numériques futurs.

Le renforcement du rôle de I'ENISA en soutien capacitaire des Etats membres et en appui au réseau de leurs équipes de réponse aux incidents parait positif et facilitera la mise en œuvre de la directive NIS. En revanche, les propositions conduisant l'agence à se substituer aux capacités des Etats-membres vont à l'encontre de leurs intérêts souverains.

La Commission des affaires européennes du Sénat saisie en application de l'article 88-6 de la Constitution a émis un avis motivé estimant que le projet de règlement ne respecte pas le principe de subsidiarité[1].

b) Les autres enjeux dans les enceintes internationales

L'ANSSI s'implique également au sein des instances internationales actives dans le domaine de la cybersécurité : l'OTAN, l'ONU et l'OCDE.

Elle développe également des relations bilatérales et multilatérales avec ses principaux partenaires de confiance, soit plus d'une quarantaine pays. L'agence a renforcé et rendu public son partenariat avec l'Allemagne autour du développement d'une industrie européenne de la sécurité numérique.

H. LE SUIVI, LE CONTRÔLE DE L'ACTIVITÉ DE L'ANSSI ET L'ÉVALUATION DE SA PERFORMANCE

L'ANSSI est rattachée au secrétaire général de la défense et de la sécurité nationale et s'inscrit logiquement dans sa mission.

Elle bénéficie dans son fonctionnement quotidien des services administratifs du SGDSN (budget, gestion des marchés, ressources humaines, etc.). Elle n'est pas pouvoir adjudicateur et ne dispose pas d'une autonomie en matière de recrutement ou de gestion de ses ressources humaines. Afin de faciliter la gestion et l'administration de l'agence, et dans un contexte de montée en puissance particulièrement rapide, une sous-

[1] http://www.senat.fr/dossier-legislatif/ppr17-079.html

direction affaires générales a été créée en janvier 2016 au sein de l'agence afin d'assurer un lien plus étroit avec ces services administratifs.

Dans un proche avenir, lorsque l'ANSSI arrivera à maturité, vos Rapporteurs estiment qu'il conviendra de s'interroger sur les moyens de lui accorder une plus grande autonomie de gestion. Elle représente aujourd'hui plus de la moitié des effectifs de l'ensemble géré par le SGDSN et un tiers des crédits.

Pour la mesure de sa performance dans la réalisation de ses activités principales ou critiques, l'agence a développé un dispositif à trois composants :

o un système de déclinaison et de pilotage de sa stratégie constitué d'un comité directeur de la stratégie et de revue du plan d'actions[1] ;

o une démarche processus, qui a permis à l'agence de décrire et partager les voies et moyens mis en œuvre pour réaliser ses missions[2] ;

o et, depuis l'été 2016, un tableau de bord général, mensuel, qui regroupe les paramètres clefs contribuant à la réalisation des objectifs de l'agence et en mesure l'efficience au moyen de 16 indicateurs. Ce tableau est analysé lors du comité de direction de l'agence afin de statuer sur les éventuelles évolutions à apporter aux actions concourant à l'atteinte de ses objectifs.

IV. LE CENTRE DE TRANSMISSIONS GOUVERNEMENTAL (CTG)

Unité militaire interarmées, placée pour emploi et sous l'autorité du SGDSN, 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 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 ;

---

[1] *Deux fois par an, le comité directeur de la stratégie fixe les orientations, fait évoluer la stratégie et rend les arbitrages nécessaires à la traduction de la stratégie en plan d'actions. La réalisation de ce dernier est suivie au cours de trois sessions annuelles de la revue du plan d'actions. Ce dispositif initié début 2016 poursuit son déploiement pour couvrir l'ensemble des niveaux managériaux.*

[2] *Cette phase, initiée en 2014, doit s'achever courant 2018. Chaque processus décrit l'enchainement des actions pour atteindre les résultats fixés et intègre un tableau de bord dédié composé de 1 à 4 indicateurs. Un dispositif additionnel, engagé courant 2017, doit permettre à chaque processus de réviser systématiquement son fonctionnement pour améliorer sa performance individuelle et celle de l'agence*

- de déployer et soutenir les systèmes interministériels sécurisés conçus par l'ANSSI sur un périmètre géographique limité.

Il assure quotidiennement l'administration de l'ensemble des communications sécurisées mis en place au niveau interministériel[1]. A ce jour, le CTG administre un parc de 1 653 stations ISIS[2] déployées sur l'ensemble du territoire métropolitain et outre-mer et de 4 082 postes TEOREM[3], répartis dans le monde. Il fournit les moyens SIC des voyages officiels du Président de la République à l'étranger et outre-mer et les missions à bord de l'avion à usage gouvernemental (AUG).

D'un effectif de référence de 181 agents[4] pour lesquels les crédits sont inscrits au budget des services du Premier ministre.

V. LE GROUPEMENT INTERMINISTÉRIEL DE CONTRÔLE (GIC)

Dans le cadre fixé par les lois du 24 juillet relative au renseignement et du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales, **le GIC est le pivot interministériel de gestion de l'ensemble des techniques de renseignement**. Il assure, pour leur mise en œuvre, un rôle de conseiller auprès du Premier ministre. Le décret en Conseil d'État du 29 janvier 2016[5] et le décret du 9 juin 2016[6] ont précisé ses attributions. Ses missions nouvelles s'accompagnent d'un changement de format et d'organisation[7].

A. LES MISSIONS DU GIC EN VOIE DE STABILISATION

1. La centralisation du circuit de validation des demandes

Le GIC assure le circuit de validation des demandes, enregistre les avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR) et les autorisations données par le Premier ministre, garantit l'homogénéité des procédures de suivi, veille à la conformité du

---

[1] *Avis de la commission des affaires étrangères, de la défense et des forces armées du Sénat n° 142 Tome IX (2016-2017) par MM., Bockel et Masseret, p. 37 et suiv.54 et suiv.*

[2] *Intranet sécurisé interministériel pour la synergie gouvernementale.*

[3] *Terminal cryptographique des réseaux étatiques et militaires.*

[4] *Le plafond d'emplois conduit à 172,5 ETP.*

[5] *https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000031940885&categorieLien=id*

[6] *https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=9EB2DC96BAFEEF5E47AA6D39C3EB0071.tpdila12v_1?cidTexte=JORFTEXT000032672675&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000032672666*

[7] *Le GIC a mis en place fin 2016 une direction de programme interministérielle pour coordonner les choix techniques et les déploiements des systèmes d'information concourant aux techniques de renseignement. Cette direction de programme soumet si besoin au cabinet du Premier ministre des propositions d'arbitrages stratégiques.*

recueil et de l'exploitation aux autorisations octroyées. Afin d'absorber la charge de travail liée à l'augmentation du nombre de demandes, de fluidifier le circuit administratif et de raccourcir les délais de traitement, le GIC a dématérialisé le circuit d'instruction de la plupart des techniques de renseignement[1].

2. L'exclusivité de la relation avec les opérateurs de communication électroniques et les fournisseurs de services de communications sur internet pour la réalisation des interceptions de sécurité et le recueil des données de connexion

Dans le cadre de ses activités « historiques », le GIC poursuit la modernisation et l'adaptation des dispositifs d'accès aux communications. Les logiciels à l'usage des services sont en constante évolution afin de faciliter l'exploitation des données recueillies.

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 participe au développement des outils et contrôle leur mise en œuvre et leur exploitation.

3. La centralisation des données recueillies par les techniques dites « de proximité [2]» opérées par les services de renseignement

Le GIC 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. Un système adapté au recueil des données techniques de localisation[3] a été déployé en priorité pour un investissement de 0,5 M€ avec un coût de maintenance annuel de 0,15 M€. Les services ne recourent donc plus à de multiples prestataires privés pour recueillir et héberger les données issues de leurs balises de géolocalisation mais uniquement aux services offerts par le GIC. Les principes retenus pour centraliser le recueil et l'exploitation des données de géolocalisation issues des balises ont été appliqués au cas, plus complexe, de centralisation des captations et d'exploitation de sons et d'images[4]. Une solution maîtrisée par

---

[1] *Il est possible depuis novembre 2016 de formuler une demande, de la faire valider par le ministre, de recueillir l'avis de la CNCTR et d'obtenir l'autorisation du Premier ministre de façon dématérialisée, en utilisant un réseau protégé, conçu et déployé par le GIC au sein des quatre ministères concernés, à Matignon et à la CNCTR*

[2] *celles de balisage (article L. 851-5 du code), celles de recueil de données de connexion par IMSI catcher (article L. 851-6 du code), celles d'interceptions de sécurité par IMSI catcher (II de l'article L. 852-1 du code), celles de captation de paroles prononcées à titre confidentiel ou d'images dans un lieu privé (article L. 853-1 du code), celles de recueil et de captation de données informatiques (article L. 853-2 du code) et celles d'introduction dans un lieu privé (article L. 853-3 du code).*

[3] *Article L. 851-5 du code de la sécurité intérieure*

[4] *Article L. 853-1 du code de la sécurité intérieure*

le GIC sera mise en service en 2018, au printemps pour les sons et à l'été pour les images. Cela représente un investissement de l'ordre de 1 M€ et une charge de maintenance annuel de 0,1 M€.

4. L'amélioration et la sécurisation de la transcription des données recueillies par les services

Le GIC accompagne les services de renseignement et de sécurité pour les 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. Présent à Paris, en banlieue, en province et outre-mer, le GIC offre aux services des emprises sécurisées depuis lesquelles ils accèdent à distance à ses entrepôts pour y exploiter les données recueillies.

Afin de faciliter le travail des enquêteurs en province, le GIC conduit avec le ministère de l'intérieur **un programme de densification de ses centres sur le territoire**. Dès 2017 et en 2018, de nouveaux centres distants seront créés, en utilisant des locaux protégés mis à disposition par la direction générale de la police nationale, mais dont l'informatique, la supervision de la sécurité, le contrôle d'accès physique et logique, relèveront du GIC.

Par ailleurs, afin de fluidifier l'accès des analystes aux transcriptions, le GIC a fait adopter en 2016-2017 un nouvel usage des niveaux de classification conduisant à admettre que la majorité des transcriptions pouvait être classifiée non plus au niveau « secret défense » mais au niveau « confidentiel défense », ce qui rend possible une transmission des transcriptions sous forme numérique aux services bénéficiaires[1] à condition que ceux-ci disposent d'un système d'information homologué au niveau « confidentiel défense ».

5. Garantir un niveau de sécurité élevé pour le transport, le traitement et la conservation des informations

Le GIC a mis en place un centre technique secondaire, conçu comme un centre de bascule de données, lequel a vocation à devenir un site de dévolution dans le cadre de son plan de continuité et de reprise. Il a donné lieu à un transfert de 1 M€ vers le ministère de la défense en 2016, et à un investissement informatique de 2,5 M€ en 2017.

---

[1] *Le GIC a contribué au développement, à titre expérimental, d'un mécanisme et des procédures de communication dématérialisée des transcriptions d'interceptions de sécurité. Ce dispositif est en cours d'évaluation depuis mi-2017. Dès qu'il sera validé, il sera étendu aux services dont les systèmes d'information sont compatibles avec les règles de protection adéquates.*

6. Rendre compte au Premier ministre de la régularité de l'emploi des techniques de renseignement

Le GIC est le conseiller auprès du Premier ministre pour la mise en œuvre des techniques de renseignement, il concourt à la traçabilité de l'exécution des techniques. À cette fin, il établit des règles et référentiels entourant leur emploi et a élaboré un guide de mise en œuvre, soumis par le Premier ministre à l'avis de la CNCTR, ainsi que des règles applicables à la manipulation des transcriptions classifiés au niveau « confidentiel défense ».

Il apporte au Premier ministre les éléments d'évaluation nécessaire même si à ce stade, la mise en place d'une mission d'audit de l'emploi, dans les services, des techniques de renseignement, recommandée par l'inspection des services de renseignement dans un rapport de février 2016, ne s'est pas encore concrétisée dans l'organigramme du GIC.

7. Être le correspondant privilégié de l'autorité de contrôle, la CNCTR, et du représentant du Premier ministre devant la formation spécialisée du conseil d'État

La Commission s'appuie sur la structure du GIC pour accéder aux données. Il doit travailler étroitement et en transparence avec elle.

Afin d'analyser la régularité de certaines demandes de mise en œuvre de techniques de renseignement, de traiter avec la CNCTR des points d'attention et d'instruire des requêtes individuelles, le GIC s'est doté d'une compétence juridique. Le Premier ministre a délégué au directeur du GIC la signature des mémoires en défense face à la formation spécialisée du Conseil d'État compétente en matière de techniques de renseignement.

B. LA CONSOLIDATION DE SON FORMAT ET DE SON ORGANISATION

Les nouvelles missions du GIC ont été accompagnées d'un changement de son format et de son organisation.

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 législatives. Cette évolution s'est traduite par :

- la publication des textes réglementaires nécessaires à la définition précise de son statut, ainsi le décret du 20 décembre 2016 portant création d'un

service à compétence nationale[1] dénommé « groupement interministériel de contrôle »;

- la révision du statut de l'ensemble de ses personnels[2] achevée en 2016 ;

- l'organisation du soutien administratif et financier par le 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. L'adossement administratif et financier[4] du groupement au SGDSN est effectif depuis la fin de l'année 2016. La gestion du personnel, du budget et des achats est réalisée avec le soutien du service de l'administration générale du SGDSN. L'organisation des différents travaux entre les deux entités est finalisée, elle se matérialisera prochainement par une convention. Elle a permis au GIC de supporter une augmentation sensible de ses effectifs opérationnels et de son activité sans augmenter les effectifs des personnels de soutien.

2. L'accroissement de l'activité du GIC

Depuis l'entrée en vigueur de la loi relative au renseignement le 3 octobre 2015, la progression de l'activité est considérable. Elle a bondi de 2015 à 2016. Les avis préalables émis, dont le nombre est égal à celui de demandes reçues, se répartissent comme indiqué dans le tableau général.

Techniques de renseignement	Avis préalables rendus
Accès aux données de connexion en temps différé (art. L.851-1)	48 208
Géolocalisation en temps réel (art. L.851-4)	2 127
Interceptions de sécurité (art. L.852-1 I)	8 538
Autres techniques	7 711

Source : CNCTR – Rapport d'activité novembre 2016

Entre 2015 et 2016 :

- le nombre d'autorisations de géolocalisation en temps réel a été multiplié par 2,5 ;
- le nombre d'autorisations de relevé de communications a été multiplié par 1,75 ;
- le nombre d'autorisations d'identification a été multiplié par 1,25 ;

---

[1] *Comme le recommandait dans son rapport pour 2015 la délégation parlementaire au renseignement http://www.senat.fr/rap/r15-423/r15-4231.pdf p.35*

[2] *Sénat - Projet de loi de finances pour 2017 Avis n° 142 (2016-2017) du 24 novembre 2016, Tome IX - par MM. Jean-Marie Bockel et Jean-Pierre Masseret p.69*

[3] *Le GIC privilégie désormais l'emploi de crédits budgétaires ordinaires et limite l'emploi de fonds spéciaux aux seules dépenses qui le nécessitent.*

[4] *En matière financière, l'emploi des fonds normaux du GIC est soumis à la charte de gestion du BOP SGDSN, effective depuis octobre 2017.*

• la progression du nombre d'interceptions de sécurité, contingenté par la loi, a conduit en 2017 le Premier ministre à revoir à la hausse le quota, après avis de la CNCTR.

Rapporté au nombre d'autorisations prononcées au dernier trimestre 2015[1], le nombre d'autorisations prononcées par trimestre en 2016 sur les techniques de renseignement dites « de proximité » (géolocalisation par balise, captation d'images, captation sonore …) a été multiplié par un facteur compris entre 2 et 6, selon la technique concernée.

Ce développement de l'activité est dû pour partie à l'encadrement de techniques dont l'usage se répand dans les services spécialisés et pour partie à l'augmentation de l'activité de lutte contre le terrorisme, priorité affichée depuis les attentats de 2015, comme le montrent les graphiques présentés dans le rapport annuel de la CNCTR[2] s'agissant des interceptions de sécurité.

Technique par technique, l'augmentation du nombre d'autorisations se poursuit à un rythme moindre mais soutenu en 2017. La progression sera de l'ordre de 15 à 30% selon les techniques à l'exception de la géolocalisation en temps réel (+ 50% environ).

Cette croissance de l'activité a des conséquences en termes d'organisation. Par exemple, le nombre de postes de travail offerts sur les différents réseaux protégés administrés et soutenus par le GIC dépasse le millier, sur une multitude d'emprises. Ce nombre va s'accroître sensiblement avec le programme de centralisation des techniques de captations de sons et d'images.

3. Les enjeux à moyen terme

Pour le GIC, les enjeux à moyen termes résident :

• dans sa capacité à **réaliser les développements informatiques nécessaires à la mise en œuvre du cadre légal**. Ceci suppose une progression régulière de ses moyens en personnel et en ressources budgétaires ;

• dans sa capacité à **s'adapter aux évolutions de ce cadre légal et aux demandes spécifiques** du Premier ministre ou de l'autorité de contrôle pour la supervision de l'activité des services, au travers de statistiques précises et détaillées. Les évolutions du cadre légal depuis l'entrée en vigueur, le 3 octobre 2015, de la loi relative au renseignement, ont été nombreuses. Si la plupart ne remettent pas en cause l'équilibre général du texte, chaque amendement a des conséquences fortes et immédiates pour le GIC qui doit faire évoluer ses systèmes informatiques et, au besoin, ses infrastructures.

---

[1] *La loi est entrée en vigueur le 3 octobre 2015*

[2] *CNCTR 1er Rapport d'activité 2015/2016* https://cdn2.nextinpact.com/medias/cnctr-premier-rapport-annuel-2015-2016.pdf *p.69 et 70*

o à titre d'exemple, un accroissement de la durée de conservation des données implique l'acquisition de serveurs supplémentaires et éventuellement de locaux aménagés pour les héberger.

o l'évolution du cadre légal d'une technique comme les interceptions sur les ondes hertziennes[1] impliquera un accroissement du nombre d'autorisations à gérer.

o la création d'un nouveau service du « second cercle » comme le bureau central du renseignement pénitentiaire[2] entraine mécaniquement la mise en place d'un nouveau circuit d'autorisation et un accroissement potentiel des postes de travail à mettre à disposition des exploitants dans les locaux du GIC, *etc*.,

o la demande du Premier ministre, dans l'esprit et la continuité de la loi sans que le législateur ne l'ait imposé formellement, de centraliser l'exploitation des techniques de renseignement de proximité et non uniquement celle de ses résultats à des fins de contrôle, conduit à des développements informatiques importants ;

o la demande de la CNCTR de statistiques sur le nombre de personnes surveillées pour la création d'un nouvel outil d'évaluation conduit au développement de programmes informatiques spécifiques pour extraire et rapprocher des données, *etc*. ;

• dans sa capacité à **évaluer correctement l'évolution de l'activité des services**, ce qui peut avoir un impact lourd en termes d'informatique mais aussi d'infrastructures.

o C'est ainsi que l'augmentation des effectifs du GIC et des sections des services de renseignement qui exploitent dans ses locaux ont conduit à ouvrir en 2016 un second site parisien dans lequel il a été initialement choisi de réunir les sections des services dits du « second cercle ». Les capacités d'hébergement offertes par ce centre sont cependant très en-deçà du besoin exprimé mi-2015 par le GIC[3]. C'est pourquoi il est indispensable, à très court terme pour accueillir les recrutements programmés, d'augmenter la capacité d'accueil, même par des solutions temporaires, pendant les deux ans nécessaires à l'aménagement d'un nouveau bâtiment. Pendant cette période, les ratios d'occupation resteront stables et les conditions de travail difficiles. Au-delà, une solution pérenne sera recherchée en remplacement du second centre parisien, pour regrouper dans un même bâtiment tous les personnels

---

[1] *Par exemple, l'article 15 de loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme concernant les interceptions de correspondances échangées au sein d'un réseau de communications électroniques empruntant exclusivement la voie hertzienne et n'impliquant pas l'intervention d'un opérateur de communications électroniques, lorsque ce réseau est conçu pour une utilisation privative par une personne ou un groupe fermé d'utilisateurs.*

[2] *Loi n° 2017-258 du 28 février 2017 relative à la sécurité publique article 35.*

[3] *Aujourd'hui le ratio d'occupation des sites parisiens est inférieur à 5 m² par poste de travail.*

chargés d'exploiter le renseignement et héberger une équipe d'agents du GIC.

o Par ailleurs, d'autres centres d'exploitation, au-delà des 27 existants[1], seront créés à partir de 2017 pour améliorer le maillage territorial et offrir aux services régionaux de sécurité et de renseignement de nouveaux points d'accès au réseau sécurisé du GIC au bénéfice direct de l'activité opérationnelle.

4. Les projections budgétaires à moyen terme

À mission constante, le GIC estime qu'un régime stabilisé pourrait être atteint en 2020. Corrélativement la prévision budgétaire devrait se stabiliser fin 2020 avec 243 ETP (hors stagiaires et personnels mis à disposition) et un budget prévisionnel de l'ordre de 45 M€ comprenant 15,5 M€ en titre 2.

5. L'évaluation de la performance du GIC

Le GIC a mis en place un indicateur synthétique pour évaluer sa performance comme le préconisait l'avis de votre commission en 2017[2]. Cet indicateur est un rapport entre le volume d'activité correspondant au nombre de demandes présentées par les services de sécurité et de renseignement, validées par le Premier ministre et le nombre d'emplois temps plein réalisés[3].

1er semestre 2016	2nd semestre 2016	1er semestre 2017
512	516	560

L'indicateur dépend de l'activité opérationnelle des services de renseignement qui demandent des techniques de renseignement. Il reflète les conséquences des évolutions techniques réalisées par le GIC qui, grâce à l'effort constant d'automatisation, améliorent la productivité de ses agents pour répondre à l'augmentation du nombre d'autorisations.

---

[1] *Certains services ont fait le choix d'exploiter depuis les centres distants, d'autres de dédier une équipe parisienne chargée d'exploiter au profit de tous les enquêteurs de terrain. La situation des emprises distantes évoluera parce qu'elles deviennent le lieu de dépôt du renseignement recueilli par les techniques de proximité, voire de son exploitation et parce que certains enquêteurs sont aujourd'hui contraints à des trajets importants pour atteindre le centre le plus proche. Un programme d'agrandissement et de construction est en cours financé à coût partagés entre le ministère de l'intérieur (infrastructure) et le GIC (équipement informatique, contrôle d'accès et fonctionnement)*

[2] *Sénat - Projet de loi de finances pour 2017 Avis n° 142 (2016-2017) du 24 novembre 2016, Tome IX - par MM. Jean-Marie Bockel et Jean-Pierre Masseret p.59*

[3] *Une pondération est appliquée au nombre de demandes validées en fonction de la charge qu'elles représentent pour le GIC.*

TITRE 2 : LES MOYENS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2018

Le budget opérationnel du programme du SGDSN dans le projet de loi s'élève à **284,7 M€** en AE et **286,4 M€** en CP **et le plafond d'emplois à 1 191 ETPT (1 113 en 2017).**

CRÉDITS DU BOP SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2018 (EN MILLIONS D'€)

	Exécution 2016 (format 2017)		LFI 2017		2018	
	AE	CP	AE	CP	AE	CP
DEPENSES DE PERSONNEL (TITRE 2)	69 559 779	**69 559 779**	85 102 152	**85 102 152**	89 672 605	**89 672 605**
Hors CAS pensions	55 334 793	**55 334 793**	66 436 865	**66 436 865**	72 014 712	**72 014 712**
CAS pensions	14 224 986	**14 224 986**	18 665 287	**18 665 287**	17 657 893	**17 657 893**
AUTRES DEPENSES (HORS TITRE 2)	172 654 850	**162 201 454**	195 673 936	**191 077 440**	195 014 060	**196 738 007**
SGDSN "programmes transverses"	9 630 790	**9 777 127**	10 510 382	**11 032 991**	9 370 346	**8 342 873**
SGDSN - CTIM	75 423 748	**73 330 048**	82 312 291	**82 749 228**	83 576 721	**83 576 721**
SGDSN - ANSSI	65 446 341	**58 370 017**	71 423 636	**65 867 595**	70 639 367	**73 390 787**
SGDSN - opérateurs	15 624 552	**15 624 552**	15 819 824	**15 819 824**	15 819 824	**15 819 824**
SGDSN - GIC	6 529 418	**5 099 710**	15 607 802	**15 607 802**	15 607 802	**15 607 802**
TOTAL SGDSN	242 214 629	**231 761 233**	280 776 088	**276 179 592**	284 686 665	**286 410 612**

Source : SGDSN / réponse au questionnaire budgétaire

Comme en 2017, son évolution continue de s'inscrire principalement :

- dans **la montée en puissance de l'ANSSI** qui bénéficiera d'une croissance annuelle de 25 ETP entre 2018 et 2022 pour atteindre 675 ETP en fin de période.

- dans **le développement des moyens nécessaires au GIC**, dont le sous-dimensionnement avait été mis en évidence, dès 2016, par le rapport de la Délégation parlementaire au renseignement[1]. Il est envisagé de faire évoluer les effectifs du groupement pour atteindre 243 ETP à la fin de l'année 2020 à raison d'une croissance de 15 ETP en 2018 et 2019 et 13 ETP en 2020.

- **le maintien des capacités d'action et de coordination des deux directions centrales du SGDSN** dans un contexte de sécurité nationale dégradé.

A l'inverse du GIC, service à compétence national[2], qui fait l'objet d'un adossement en gestion sur le BOP SGDSN, dont il est une unité opérationnelle, l'ANSSI qui représente aujourd'hui près de 60% des effectifs budgétaires (572,8/963,5 ETP), et plus de 40% des crédits de l'unité opérationnelle SGDSN (opérateurs compris) et relève du même statut juridique, ne constitue pour autant ni un BOP autonome, ni une unité

[1] *Délégation parlementaire au renseignement - Rapport d'activité pour 2015 p. 35 et suiv. - février 2016* http://www.senat.fr/rap/r15-423/r15-4231.pdf

[2] *Décret n°2016-1772 du 20 décembre 2016*

opérationnelle. Au sein du SGDSN, le service d'administration générale assure l'ensemble des rôles et fonctions comptables et budgétaires pour l'ensemble des directions et services soutenus dont fait partie l'ANSSI.

Vos rapporteurs regrettent que les crédits de l'ANSSI ne fassent pas l'objet d'une présentation distincte dans le PAP. Sans doute, peuvent-ils recevoir cette information dans les réponses aux questionnaires budgétaires, mais ce serait un moyen de distinguer d'emblée les efforts en matière de cyberdéfense et les moyens dévolus aux autres missions du SGDSN, assurant ainsi à nos concitoyens un meilleur compte rendu de l'emploi des deniers publics. Ils demandent à ce que la maquette de présentation du programme 129 soit modifiée dans ce sens.

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 2018

	LFI 2017		PLF 2018	
	ETP	ETPT	ETP	ETPT
ANSSI	547,8		572,8	
CTG	172,5		172,5	
SGDSN hors ANSSI et CTG	218,2		218,2	
TOTAL SGDSN	938,5		963,5	
GIC	200,6		215,6	
TOTAL du BOP SGDSN	1 139	1 128	1 179	1 191

Source : SGDSN / Réponse au questionnaire budgétaire. Les crédits du titre 2 sont donnés à titre indicatif et dépendent de l'agrégation réalisée au niveau de la mission.

1. L'évolution des emplois et des crédits de personnel

Sur la période 2010-2017, l'évolution des crédits du SGDSN est principalement marquée par l'augmentation des effectifs de l'ANSSI[1], et plus récemment ceux du centre de transmissions gouvernemental (CTG)[2][3] ainsi que ceux du GIC[4], dont la totalité des effectifs est désormais retracée sous le plafond d'emplois du SGDSN.

Le plafond d'emplois du SGDSN a subi une diminution globale de 25 emplois sur la période considérée, avec une décélération de cette tendance les trois dernières années (-1 ETP chaque année, stabilité prévue en 2018).

---

[1] *460 ETP en 2016, 497,8 ETP en socle au 1er janvier 2017, 50 ETP en création en 2017*

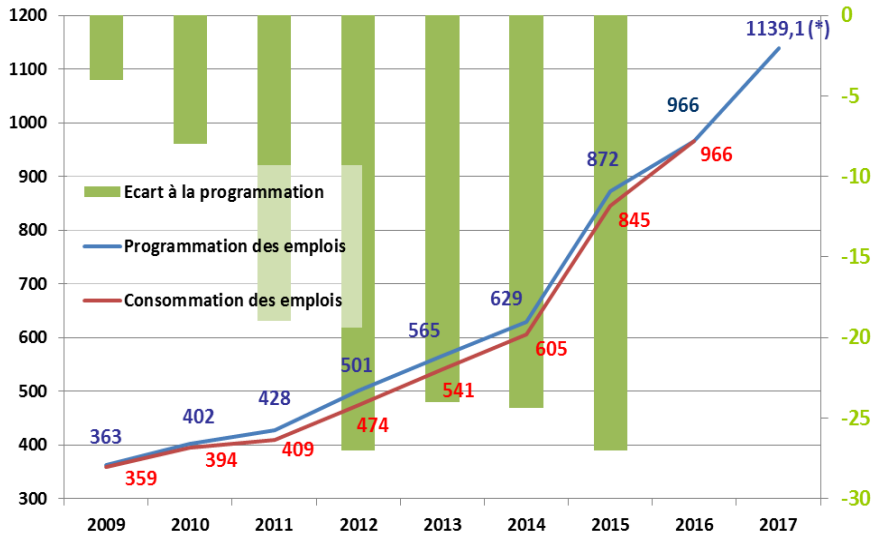
[2] *Décret du 12 juin 2014*

[3] *qui représentent 170,5 ETP en socle au 1er janvier 2017*

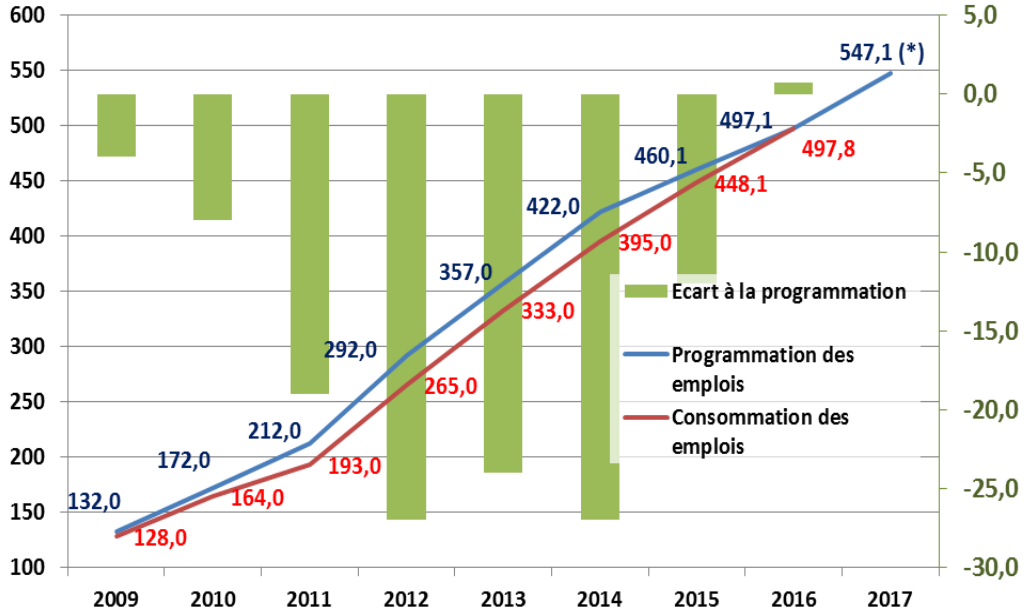
[4] *82,6 ETP en socle au 1er janvier 2017, avec une cible à 200,6 ETP à la fin de cette année, 83 emplois transférés en 2016, puis en 2017 et 35 ETP en schéma d'emploi*

Les graphes ci-après synthétisent l'évolution des emplois en programmation et en exécution, à périmètre constant, sur la période 2010-2017 (en ETP).

Situation générale SGDSN



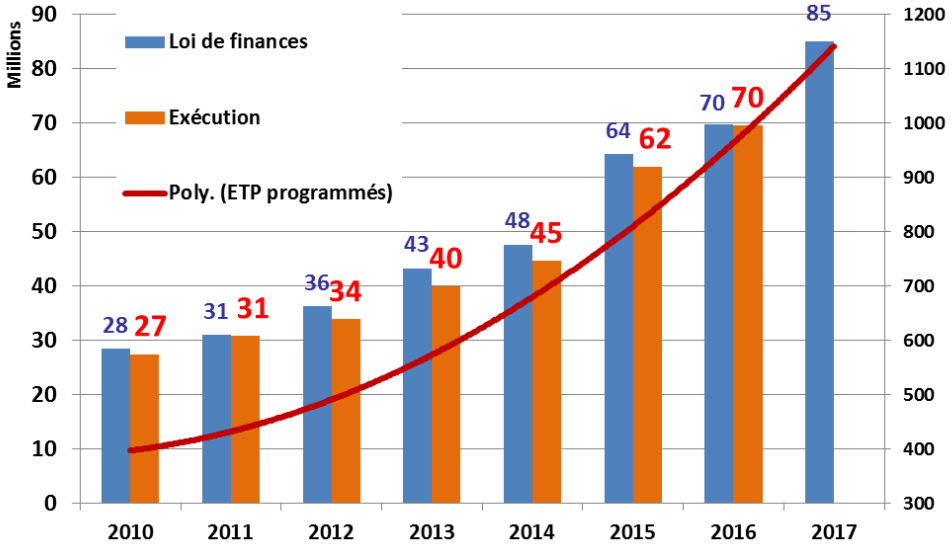
Situation particulière de l'ANSSI



(*) Cible en programmation 2017 (ETP)

Source : SGDSN réponse au questionnaire parlementaire

L'évolution des crédits suit celle des effectifs et des changements de périmètre (CTG, GIC). Ainsi, en 2017, 85,1 M€ de crédits ont été votés pour le SGDSN[1] (70,7 M€ en 2016), dont 18,7 M€ sur le CAS Pensions.



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 en PLF 2018

En 2017, l'ANSSI bénéficie d'un schéma d'emplois de +50 ETP, ce qui devrait lui permettre d'atteindre à la fin de cette année près de 550 ETP. L'évolution se poursuit à raison de + 25 ETP par an en 2018.

Il est prévu de faire évoluer de 15 ETP les effectifs du GIC, qui devraient s'établir à 200 ETP à la fin de 2017 et à 215 à la fin de 2018.

Sous réserve de la consolidation des crédits du titre 2, l'estimation de la masse salariale du SGDSN en 2018 est de 89,67 M€, dont 17,66 M€ sur le CAS Pensions. Cette hausse de 5,4 % s'explique essentiellement par[2] :

- le schéma d'emplois de l'ANSSI (+25 ETP) et du GIC (+15 ETP), représentant au total 20 ETPT sur le plafond d'emplois ;
- et l'effet report des emplois créés en 2017 (41,7 ETPT).

Cette estimation de masse salariale intègre également, au titre des mesures catégorielles nouvelles, une demande de 0,46 M€ destinée à la revalorisation du régime indemnitaire des agents de l'ANSSI[3].

---

[1] *La réserve de précaution est de 0,4 M€.*

[2] *Elle conduira à un plafond d'emplois à l'échelle du SGDSN de 1 191 ETPT.*

[3] *Cette revalorisation s'inscrit dans l'esprit de la circulaire du Premier ministre en date du 21 mars 2017, qui invite notamment chaque employeur à conduire* «une politique indemnitaire permettant de valoriser les métiers numériques et SIC pour fidéliser les compétences rares».

B. LE SGDSN : UNE VIGILANCE A GARDER SUR L'ORGANISATION DES FONCTIONS DE SOUTIEN

Le SGDSN 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 son « cœur historique ».

Dans son précédent rapport, votre Commission s'était inquiétée de la diminution des effectifs de la fonction support du SGDSN dans un contexte de développement de structures supportées et estimait qu'il devra, en conséquence, veiller à renforcer cette fonction pour assurer efficacement le pilotage et la coordination de l'ensemble. Le ratio est passé de 15,6% en 2009 à 7,43% en 2016. Ce faisant une partie des fonctions supports ont été développées au sein des entités elles-mêmes.

Dans le projet de loi de finances pour 2018 les renforts en personnel étant fléchés en direction de l'ANSSI et du GIC, le SGDSN stricto sensu conserve le même schéma d'emploi.

Vos rapporteurs estiment que cette situation doit faire l'objet d'une attention vigilante. Pour assurer un renforcement du support, deux solutions peuvent être envisagées, soit un renforcement au sein du service de l'administration générale du SGDSN, soit, comme c'est le cas depuis plusieurs années, celui des fonctions supports au sein des entités soutenues, ce qui présente l'avantage d'une simplification dans la gestion quotidienne, tout en conservant le niveau de supervision stratégique du SGDSN.

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 doit être poursuivi en 2018. En effet, elle doit non seulement assurer ses missions habituelles dont la charge est en croissance permanente, notamment en matière de traitement des attaques informatiques, mais 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 enfin contribuer aux réponses apportées aux besoins croissants de sécurisation des entreprises et des particuliers.

Sans anticiper sur les conclusions de la Revue de la stratégie Cyber, actuellement conduite par le SGDSN, et au vu des conclusions de la Revue stratégique de défense et de sécurité nationale publiée en octobre 2017, le renforcement des moyens de l'ANSSI sera à l'ordre du jour des prochaines années, compte tenu du développement des menaces et de la croissance des enjeux en raison de la numérisation croissante des activités humaines.

La croissance des effectifs a d'ores et déjà permis à l'agence de passer de 122 ETP en 2009 à 547 ETP fin 2017. Les évolutions opérationnelles

prévisibles à l'horizon 2022 conduisent à autoriser le recrutement de 25 ETP an sur le schéma d'emplois. A la fin de l'année prochaine, l'agence devrait ainsi compter à 572 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. Cet objectif ne sera atteint qu'en 2022 (675 ETP) ce qui n'est sans doute pas à la hauteur des enjeux.

Vos rapporteurs espèrent que la revue de stratégie cyber constituera un levier efficace pour solidifier le schéma d'emploi de l'ANSSI compte tenu de l'intensification de la menace et du développement attendu de ses missions.

Sous-directions	**Effectifs fin 2017**	**Effectifs fin 2018**
Centre opérationnel de la SSI (COSSI)	176	184
Sous-direction expertise (SDE)	148	155
Systèmes d'information sécurisés (SIS)	101	106
Relations extérieures et coordination (RELEC)	72	75
Sous-direction affaires générales (SDAG)	27	28
Autres	23	24
Effectif total ANSSI	**547**	**572**

Source : SGDSN – réponse au questionnaire parlementaire

Dans son précédent rapport[1], votre commission a présenté la structure d'emploi de l'ANSSI, faisant ressortir la jeunesse des personnels employés (2/3 de moins de 40 ans) et la présence très largement majoritaire (77% de contractuels). En effet, les profils recherchés par l'ANSSI sont rares dans la fonction publique. Les orientations stratégiques de l'agence précisées dans un document annuel de politique des ressources humaines sont :

- le renforcement de l'attractivité et la fidélisation des agents ;
- l'optimisation de la gestion des ressources humaines ;
- l'amélioration de la lisibilité et de la cohérence des parcours professionnels.

La montée en puissance reste un défi structurel de l'agence qui doit également pourvoir au *turn over* (15,5% en 2016[2]) important de ses agents dont nombre sont des contractuels. Elle doit à la fois recruter en nombre et maintenir la qualité de ce recrutement.

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 est plus problématique compte tenu des rémunérations offertes par le secteur privé, malgré l'existence de procédure permettant la transformation des CDD

[1] Sénat - Projet de loi de finances pour 2017 Avis n° 142 (2016-2017) du 24 novembre 2016, Tome IX - par MM. Jean-Marie Bockel et Jean-Pierre Masseret p.66 à69

[2] *Un taux légèrement inférieur à ceux observés dans le domaine d'activité dans le secteur privé.*

en CDI et la relative 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 les problèmes de recrutement qu'a pu rencontrer l'ANSSI lors de sa première phase de montée en puissance sont en partie résolus. Néanmoins, une attention vigilante doit être maintenue parce que le vivier de formation initiale reste faible au regard des besoins d'ingénieurs spécialistes de la sécurité informatique et du cyber tant de l'ANSSI, que de l'ensemble des administrations publiques et du secteur privé et parce que le ralentissement des créations de postes au sein de l'ANSSI ne paraît pas cohérent avec le développement probable de ses missions dans les prochaines années. Enfin il demeure souhaitable qu'une certaine souplesse continue à être recherchée 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. De ce point de vue, la circulaire du Premier ministre en date du 21 mars 2017, qui invite notamment chaque employeur à conduire « *une politique indemnitaire permettant de valoriser les métiers numériques et SIC pour fidéliser les compétences rares* » constitue une avancée importante.

À plus long terme, une politique active de développement de filières de formation en écoles d'ingénieurs et en universités doit être conduite. Dans son précédent rapport, votre commission a salué l'engagement de l'ANSSI dans une politique de labellisation des formations universitaires, mais estimait que cet effort devait 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. Ils espèrent que cet objectif sera développé dans le cadre de la Revue stratégique cyber et décliné sous forme d'orientations concrètes à conduire dans les prochaines années.

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

1. Le GIC assure désormais la gestion administrative de son personnel et bénéficie de son adossement au BOP SGDSN

La totalité des agents du GIC[1] a été intégrée, détachée ou mise à disposition au sein du SGDSN au 1er janvier 2017[2]. Ayant ainsi rompu le lien

[1] *à l'exception des 10 gendarmes assurant la sécurité du centre principal du GIC, mis à disposition par la gendarmerie nationale.*

[2] *Sur le dispositif d'intégration réalisé en 2016 voir Sénat - Projet de loi de finances pour 2017 Avis n° 142 (2016-2017) du 24 novembre 2016, Tome IX - par MM. Jean-Marie Bockel et Jean-Pierre Masseret p.69*

administratif historique avec la DGSE, le GIC est désormais pleinement autonome par rapport aux services de renseignement.

Dès mai 2015, le GIC avait conduit une première étude montrant le besoin d'une augmentation progressive de ses effectifs, visant l'atteinte d'un effectif cible de 220 ETP en 2020 et 14 M€ de crédit en titre 2. Outre le fait que les effectifs du groupement étaient devenus insuffisants pour assurer ses missions historiques[1], l'estimation prenait en compte les nouvelles missions qui seraient confiées au GIC par la loi sur le renseignement, alors en projet.

Dans son avis sur le PLF 2017[2], votre commission estimait que « *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* **«** et souhaitait « *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 exécution, le nombre des recrutements a été de 38 et le nombre de départ de 13, essentiellement pour des départs en retraite – le *turn over* pour départ en retraite du GIC est de l'ordre de 5% par an – soit un déficit de 10 par rapport au schéma d'emploi. **Vos rapporteurs considèrent que ces emplois sont nécessaires et que le défaut de recrutement résulte des difficultés intrinsèques aux catégories de personnel recherchées et aux conditions spécifiques d'embauche, en conséquence ils devront faire l'objet d'une mesure de report sur le schéma d'emploi de 2018**.

Un nouvel arbitrage a conduit à revoir la cible ainsi que le rythme de progression des recrutements. Au vu de l'augmentation considérable du recours aux techniques de renseignement par les services en 2016, il est prévu de faire évoluer les effectifs du GIC. Ils devraient s'établir à 200 ETP à la fin de 2017, pour atteindre 243 ETP à la fin de l'année 2020 (+ 15 ETP en 2018, + 15 ETP en 2019 et + 13 ETP en 2020).

	2015	2016	2017	2018	2019	2020
En ETP *	132	160	200	215	230	243

** y compris, à partir de 2017, les gendarmes chargés de la sécurité sur le nouveau site parisien (9 ETP).*

[1] *Mise en œuvre des interceptions de sécurité et recueil des données de connexion auprès des opérateurs.*

[2] *Sénat - Projet de loi de finances pour 2017 Avis n° 142 (2016-2017) du 24 novembre 2016, Tome IX - par MM. Jean-Marie Bockel et Jean-Pierre Masseret p.72*

Cette évolution prend également en compte la création d'un nouveau service habilité, le bureau central du renseignement de l'administration pénitentiaire, la mise en œuvre des techniques les plus innovantes autorisées par la loi du 24 juillet 2015 et la nécessité de doubler la permanence du GIC pour accompagner l'augmentation des effectifs des sections d'exploitation des services de renseignement

Le montant des crédits inscrits dans le PLF 2018 au titre 2 de l'unité opérationnelle GIC s'élèvent à 12,559 M€[1] (10,907 M€ en PLF 2017) soit une progression de 15,1% et devraient atteindre 15,5 M€ en 2020.

Vos rapporteurs ne peuvent que se féliciter de cette adaptation aux besoins. Il reste cependant à réaliser cet objectif et notamment à pourvoir les 25 emplois ouverts en 2018 (10 au titre du reliquat 2017 et 15 au titre du schéma d'emploi 2018) et au remplacement de la dizaine de collaborateurs qui quitteront le GIC durant cette période.

La réalisation de cet objectif comme la transformation progressive du GIC suppose une politique des ressources humaines active.

2. La politique des ressources humaines du GIC

Elle obéit à deux impératifs :

- quantitatif, pour répondre à l'évolution des missions et à l'augmentation sensible des demandes de mise en œuvre de techniques de renseignement ;

- 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[2].

Pour mener ses nouvelles missions d'audit des services dans le cadre de la centralisation du renseignement, issu des techniques de recueil de proximité, le groupement doit développer de nouvelles compétences, constituer des équipes et élaborer des procédures inédites. Il a dû aussi se doter d'une compétence juridique de haut niveau.

Cette évolution est en cours. Une analyse de la structure des effectifs du GIC de 2011 à 2016 montre que :

- la proportion d'agents de catégorie A ou officier est passée de 12 à 26% les catégories B et C baissant à due concurrence ;

---

[1] *Dont 8,572 M€ de rémunérations d'activité (7,4 en PLF 2017), 3,727 de cotisations en contributions sociales y compris les cotisations au CAS Pensions (3,3 en 2017) et 0,291 de prestations sociales et allocations diverses (0,17 en 2017).*

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

- la proportion du personnel militaire est passée de 43 à 24% à raison de l'impossibilité pour le ministère des armées de proposer des personnels militaires, dotés des qualifications requises, en nombre croissant pour soutenir le développement du GIC. Ceci a conduit parallèlement à une hausse sensible des personnels civils contractuels de 36 à 53% ;
- enfin, les moins de 35 ans sont passés de 11 à 25%.

Les profils recherchés par le GIC

+ des ingénieurs informatiques de haut niveau (développeurs et chefs de projet), spécialistes des télécommunications, pour lesquels le principal handicap est le niveau de rémunération servie par rapport aux postes équivalents dans le secteur privé, mais aussi la durée du processus d'habilitation – tous les personnels du GIC sont habilités au niveau « secret défense » - qui est difficilement compatible avec la disponibilité des candidats potentiels.

+ des opérateurs exploitants pour lesquels la publicité des vacances de poste est, par construction, discrète et peu explicite ce qui ne facilite pas le recrutement et pour lesquels la procédure est longue en raison de la priorité donnée par le contrôle budgétaire et comptable ministériel à la mobilité au sein de la fonction publique avant d'ouvrir la possibilité de recruter des contractuels.

Vos rapporteurs estiment que le contrôle budgétaire et comptable ministériel des services du Premier ministre devrait en l'espèce faire preuve de souplesse tant dans la définition des plafonds de rémunération que pour l'accélération des procédures de recrutement. La transformation et la modernisation du GIC est en effet un enjeu important pour la mise en œuvre efficiente de la politique du renseignement. Ce processus de transformation devra être suivi et piloté avec toute l'attention requise. Un renforcement de la fonction RH au sein du GIC devra accompagner cette montée en puissance.

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

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

1. Les crédits hors titre 2 en 2017

En 2017, 181 M€ d'AE et 176,5 M€ de CP ont été ouverts en loi de finances pour le BOP. Ceci correspond aux ressources notifiées et intègre une mise en réserve de 8%, programme interministériel compris, exception faite des subventions pour charges de service public versées aux opérateurs pour lesquels un taux réduit a été retenu (voir infra p. 65 et suiv.).

S'agissant des mouvements réglementaires de crédits, le SGDSN prévoit le transfert de 73,4 M€ d'AE et de 74,5 M€ de CP en 2017 par deux décrets publiés respectivement le 7 mai.

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 notamment dans le domaine de la sécurité des systèmes d'information. Il est ainsi prévu de contribuer principalement aux financements :

- d'opérations de développement et de maintien des capacités techniques interministérielles décidées en comité de pilotage « CTIM » par le cabinet du Premier ministre (61,7 M€ en AE et 64,1 M€ en CP) ;

- du financement des produits de sécurité sous maitrise d'ouvrage déléguée à la direction générale de l'armement (10 M€ d'AE et de 2,7 M€ de CP) ;

- du financement du bâtiment 13 de l'Ecole militaire, pour les besoins de l'INHESJ et du CSFRS (1,7 M€ en AE et CP) ;

- du financement d'un centre de données sécurisé destiné à l'ANSSI (6 M€ de CP).

Un troisième décret de transfert sera instruit à l'automne 2017. Il intéressera le ministère de la défense, notamment au titre des produits de sécurité, et le ministère de l'intérieur pour les moyens de lutte NRBC.

À ces mouvements réglementaires s'ajoute la mise à disposition de 0,8 M€ d'AE et de 1,1 M€ de CP pour le financement du projet de téléphonie mobile sécurisée interministérielle.

Il convient enfin de noter que :

- le budget du SGDSN a fait l'objet d'une annulation de crédits de 5,8 M€ en AE et en CP dans le cadre du décret n° 2017-1182 du 20 juillet 2017 ;
- l'INHESJ a bénéficié d'un abondement complémentaire de 70 000 € en AE et en CP pour le financement du conseil scientifique sur les processus de radicalisation.

2. Les crédits hors titre 2 en PLF 2018

Le PLF 2018 prévoit l'ouverture de 163,58 M€ d'AE et de 165,31 M€ de CP pour l'ensemble SGDSN/ANSSI (hors GIC et subvention aux opérateurs). Cela représente, en CP, une évolution de l'ordre de 3,5% par rapport à la LFI 2017. Les crédits ouverts seront essentiellement mobilisés sur le développement de la cyberdéfense et la résilience des communications gouvernementales.

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 représentent une part importante du budget de l'agence et implique l'utilisation de décrets de transfert annuels entre programmes en lien avec la DGA. Le budget s'élève à 6,55 M€ en AE et 11,46 M€ en CP pour 2018. Le lancement d'un programme de développement d'un nouveau chiffreur, à hauteur de 5,22 M€ en AE est également prévu ;

- 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. Afin de permettre l'adoption rapide et massive de produits recommandés, l'agence recourt à l'achat de licences globales pour les administrations. Ces licences qui sont incluses dans les dépenses pour immobilisation incorporelles s'élèvent à 4 M€ en AE et 4,75 M€ en CP.

Les autres dépenses couvrent :

- Les équipements des laboratoires nécessaires à l'expertise techniques : 2,31 M€ en AE et 2,14 M€ en CP.

- l'achat des logiciels ou des matériels nécessaires aux maquettages des solutions envisagées dans le cadre de la mission d'assistance technique de l'agence et la prise en charge partielle du financement de la sécurité du RIE : 2,03 M€ en AE et 2,13 M€ en CP.

- des achats d'équipement et de prestations informatiques pour les besoins de la gestion de la disponibilité de ses capacités informatiques propres et de celles du SGDSN pour un montant de 20 M€ en AE et 19,72 M€ en CP[1].

- le développement et le soutien des réseaux et systèmes sécurisés interministériels conduisent à des dépenses d'un montant de 10,71 M€ en AE et 9,71 M€ en CP.

a) L'ANSSI représente une part importante des crédits hors titre 2

La dotation de l'ANSSI (73,39 M€ en CP et 70,64 en AE) est consolidée par rapport à 2017 (66,87 M€ en CP et 72,43 en AE).

Hors ANSSI, le SGDSN dispose de 91,9 M€ en CP pour 2018, soit une légère diminution de 2% que l'on retrouve très atténuée en AE (-0,1%) et s'élèvent à 92,9 M€. 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 8,34 M€ en 2018 contre 11,03 M€ en CP et subissent une érosion sensible (-24%). 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

[1] *Il est dommage que la présentation dans le PAP ne fasse par apparaître clairement la répartition des achats entre ce qui revient au SGDSN stricto sensu et ce qui revient à l'ANSSI.*

nationale transférés en cours d'exercice vers le ministère de la défense dont l'enveloppe progresse légèrement (+1,5% en AE et 1% en CP) et s'établissent à 83,57 M€ en AE et en CP.

Malgré la forte diminution de ces moyens, le SGDSN estime que le budget des deux directions (protection et sécurité de l'État, affaires internationales, stratégiques et technologiques) sera maintenu à un niveau permettant son intervention dans l'ensemble des actions interministérielles de défense et de sécurité. Un effort particulier sera entrepris dans le domaine du soutien aux industries de sécurité, qui s'avère aujourd'hui insuffisant.

b) Crédits de fonctionnement de l'ensemble SGDSN/ANSSI (hors GIC et subvention aux opérateurs)

Les crédits de fonctionnement s'élèvent à périmètre courant (hors GIC) à 62,4 M€ d'AE et 64,7 M€ de CP et sont destinés à couvrir principalement les dépenses et les actions suivantes :

- les communications électroniques sécurisées (17,2 M€ d'AE et 15,5 M€ de CP) : achat de matériel (réseaux, sécurité, postes de travail et petit matériel) et maintien en conditions opérationnelles des systèmes d'information et transfert de compétence nécessaire à leur utilisation ;

- l'acquisition de logiciels et abonnements à des services de veille et d'analyse technique des menaces (vulnérabilités logicielles, codes malveillants) pour le COSSI, ainsi que la mise en place d'une plateforme d'échange par le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques, pour un montant de 2,5 M€ en AE et 2,2 M€ en CP ;

- la politique d'expertise scientifique et technique et le développement de produits de sécurité (8,6 M€ en AE et 8,8 M€ en CP) ;

- la coordination territoriale, les relations internationales et la politique de sensibilisation de l'ANSSI (2,1 M€ en AE et 2 M€ en CP) ;

- le fonctionnement des liaisons officielles (maintien en conditions opérationnelles, achat de petits équipements, formation métier sur les réseaux hautement protégés, moyens sécurisés de communication, soutien et exploitation du système d'information… 9,6 M€ en AE et 10,1 M€ en CP) ;

- les affaires internationales et stratégiques en matière de lutte contre la prolifération et de contrôle des exportations de matériels de guerre (0,3 M€ en AE et 0,4 M€ en CP) ;

- une enveloppe de 5,2 M€ en AE et 4,8 M€ en CP dédiées aux programmes interministériels de lutte contre la menace nucléaire, radiologique, biologique, chimique et explosive (NRBC-E), ainsi que d'autres programmes liés à la lutte contre l'utilisation malveillante de drones ou au réseau gouvernemental d'alerte. De même, seront pris en charge la réalisation d'exercices nationaux de simulation de gestion de crise afin de garantir la continuité de l'Etat.

Les autres dépenses de fonctionnement courant sont estimées à 8,3 M€ d'AE et 7,9 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.

Vos rapporteurs regrettent que la présentation de ces dépenses dans le PAP ne s'appuie pas sur une nomenclature pérenne, ce qui empêche toute comparaison d'une année sur l'autre à l'exception de quelques rubriques.

- S'agissant des dépenses immobilières :

o 6,8 M€ d'AE et 11,2 M€ de CP sont destinés aux dépenses immobilières des différents sites recouvrant les loyers, charges, taxes, dépenses d'énergie et fluides, ainsi que les services aux bâtiments (maintenance, sécurité, nettoyage) ;

o 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].

c) Les versements des subventions pour charges de service public des opérateurs

Les subventions pour charges de service public des opérateurs sous tutelle du SGDSN sont maintenues 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€.

d) 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 99,9 M€ d'AE et 99,2 M€ de CP pour 2018, ils ont vocation à financer les projets suivants :

- 14,5 M€ d'AE et 10 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 des armées et notamment le développement des programmes de « Chiffrement IP » et « Crypsis NG » : programmes ayant pour objet d'assurer la protection de flux classifiés, véhiculés à travers internet ;

- 8,2 M€ en AE et 7,4 M€ en CP sont prévus pour l'acquisition de matériel de sécurité de type chiffreurs, serveurs, ainsi que d'équipement de mesure électronique et électromagnétique pour les laboratoires du COSSI. Ces équipements

[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 jusqu'en 2019 inclus.*

serviront notamment aux réseaux Horus (visioconférence sécurisée) ainsi qu'aux salles serveurs du data center en construction ;

- 2,7 M€ d'AE et 2,2 M€ de CP seront destinés à l'achat de licences et logiciels spécifiques à l'investigation numérique, à la détection et au développement de la plate-forme de tests de robustesse de systèmes industriels ;

- 1,1 M€ en AE et 1 M€ CP sont prévus pour des actions à travers des conventions conclues avec le laboratoire central de la Préfecture de police dans le domaine des matériaux énergétiques, avec l'Institut franco-allemand de Saint-Louis en matière de recherche sur les explosifs artisanaux et avec la direction générale de la police nationale pour l'acquisition de matériels dédiés à l'intervention sur des engins suspectés de contenir des agents biologiques ou chimiques ;

- Enfin, 2,6 M€ d'AE et 7,8 M€ de CP sont liés à la poursuite de travaux immobiliers engagés : sécurisation de l'alimentation électrique, production de froid, financement de la construction du nouveau centre de données sécurisés de l'ANSSI (6 M€)[1] ;

- Par ailleurs, une dotation de 70,8 M€ d'AE et en 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.

e) Les dépenses d'intervention

Le SGDSN a prévu une dotation de 3,3 M€ en AE et 3,4 M€ en CP pour les dépenses suivantes :

- 1,3 M€ en AE et 1,5 M€ en CP destinés au fonds unique interministériel (FUI) dans le cadre du cofinancement de projets de recherche innovants, ainsi qu'aux travaux de recherche menés par l'Agence nationale de la recherche (ANR) en matière de sécurité et enfin au Haut comité français pour la défense civiles (HCFDC) ;
- 1,8 M€ en AE et 1,7 M€ en CP attribués à différents projets et initiatives dans le cadre d'une convention relative à la cybersécurité du futur, dans le cadre de la convention conclue avec Bpifrance, ou dans le cadre de groupement d'intérêt public (GIP dédié au développement et à la promotion des entreprises, GIP pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance) ;
- 0,2 M€ en AE et en CP de subvention versée au CSFRS.

[1] *Le coût global de l'opération est aujourd'hui estimé à 25,55 M€. Un premier transfert de 18,2 M€ en AE a été transféré au ministère de l'intérieur responsable du projet et 6 M€ en CP sont inscrits qui feront l'objet d'un transfert au profit du programme 216 « conduite et pilotage des politiques de l'intérieur ». Les CP sont progressivement décaissés jusqu'en 2019*. Voir encadré supra p. 27

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

Le montant prévu au PLF 2017 s'élevait hors titre 2 à 16,6 M€ en AE et en CP (8,8 en titre 3 et 7,8 en titre 5). Compte tenu de la mise en réserve et des annulations intervenues en cours d'année, le montant consommé devrait, sauf mesure de dégel s'élever à 12,5 M€ en crédits de paiement. La GIC a dû, en conséquence, différer certaines commandes concernant la modernisation de son *data center*.

CP	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
LFI 2016 exécutée (*)	4,5	8,05		8,05	
PLF 2017	10,9	8,8	7,8	16,6	
LFI 2017 (**)	11,5	3,44	12,17	16,61	
		1,0			
PLF 2018	12,6	3,4***	12,2***	15,6	

En M€
(*) Tous BOP confondus : SGDSN (UO GIC et UO SGDSN) et Soutien de la DASF
(**) UO GIC et UO SGDSN
(***)Titre 3 : 4,8 en AE, Titre 5 : 10,8 en AE

Pour mémoire, on rappellera qu'avec l'évolution de ses missions dans le cadre des lois du 24 juillet et du 30 novembre 2015, le GIC est financé à titre principal par des crédits généraux et pour une partie plus réduite de son activité par des fonds spéciaux qu'il appartient à la commission parlementaire de vérification des fonds spéciaux de contrôler.

Pour 2018, le budget HT2 en fonds normaux du GIC (**15 607 802 € en AE et en CP**) tient compte de l'impact de la loi relative au renseignement et des dispositions règlementaires d'application[1] et de la forte augmentation d'activité liée à la lutte antiterroriste. Sont inscrits en titre 3, 4,808 M€ en AE et 3,440 M€ en CP, et au titre 5, 10,767 M€ en AE et 12,168 en CP.

1. Les crédits de fonctionnement

Les crédits de fonctionnement courant (4,8 M€ en AE, 3,44 M€ en CP) ont vocation à financer le maintien en conditions opérationnelles des différents systèmes d'information et réseaux existants, ainsi que le raccordement au réseau interministériel de l'État. Ces crédits couvrent

[1] *Notamment le décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.*

également le fonctionnement courant de la structure (frais de mission, formation, action sociale, équipement et documentation) ainsi que les dépenses immobilières de types fluides, charges et services aux bâtiments (1,4 M€ en AE et 1,1 en CP).

2. Les crédits d'investissement

Les crédits d'investissement se répartissent en :

- des dépenses pour immobilisations incorporelles pour 6,6 M€ en AE et 6,3 en CP qui se rattachent notamment aux projets d'administration et de supervision des systèmes d'information, ainsi qu'aux obligations créées par la loi du 24 juillet 2015 et ses décrets d'application[1] ;

- des dépenses pour immobilisations corporelles à hauteur de 4,3 M€ en AE et 5,9 en CP qui concernent notamment l'achat d'équipements pour la réalisation de plateformes supports, la rénovation du cœur du réseau informatique et l'extension du *data center*.

Elles 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.

La montée en puissance du GIC conduit à une mise à niveau des systèmes d'information :

- le développement des outils d'administration et d'hypervision développés par le GIC pour la mise en œuvre du cadre légal, au profit des services de renseignement, du Premier ministre et de l'autorité indépendante. L'utilisation de ces systèmes est croissante et leur disponibilité indispensable ; ce chantier est lourd car il concerne différents réseaux et 2 000 utilisateurs actuellement (agents des services de renseignement) ;

- l'extension du centre de données du GIC, rendue indispensable par les nouveaux systèmes d'information à héberger (exigence légale de centralisation du renseignement, dématérialisation du circuit de validation des demandes de techniques de renseignement) et l'augmentation des données stockées au GIC (augmentation des durées de rétention des informations, centralisation des techniques de renseignement) ;

- la sécurisation des liens internet permettant le recueil par le GIC des données issues des techniques de renseignement nouvellement encadrées par la loi. Le transfert de plus en plus important de données par le biais d'internet nécessite des passerelles sécurisées et performantes, dotées de systèmes de supervision d'éventuelles cyberattaques ;

---

[1] *Notamment le financement du programme de centralisation du renseignement qui va se poursuivre afin de couvrir l'ensemble des techniques de renseignement.*

- les plateformes de développement et de recette.

L'hébergement 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 quasiment doublé à l'horizon 2020 par rapport à 2015, pourvoir à l'aménagement de ses infrastructures. Ces besoins nécessiteront d'attribuer au GIC de nouveaux locaux à très court terme, pour la période 2018-2020, puis à long terme pour une solution pérenne.

La mise en œuvre rapide des dispositions de la loi sur le renseignement a imposé au GIC une profonde réorganisation de ses modes de fonctionnement budgétaires et financiers. Vos rapporteurs estiment nécessaire que les modalités techniques d'adossement du GIC au SGDSN soient rapidement stabilisées de façon à entamer la gestion de l'exercice 2018 sur des bases solides. Ils souhaitent que le GIC puisse assurer une programmation pluriannuelle de ses investissements et soit en mesure, dans sa phase de montée en puissance, si cruciale pour la mise en œuvre efficiente des lois de 2015, de les conduire sans retard tout en conservant la réactivité dont il a su faire preuve dans un contexte général d'accroissement de ses missions, et d'intensification de son activité. Pour ce faire, ils estiment important que le GIC puisse consolider ses fonctions supports dans le domaine budgétaire et comptable et dans le domaine de la gestion de ses ressources humaines.

C. DES OPÉRATIONS IMMOBILIÈRES À CONDUIRE D'ICI 2022

Un schéma directeur des travaux d'infrastructure établit la programmation des opérations immobilières sur les différents sites occupés par le SGDSN pour les prochaines années (2018-2022).

Les objectifs poursuivis intègrent l'élargissement des missions du SGDSN et l'augmentation de ses effectifs, notamment ceux de l'ANSSI et du GIC. Ils doivent notamment répondre à des besoins techniques grandissants et aux contraintes inhérentes à la sécurité tout en préservant la richesse architecturale et patrimoniale de l'Hôtel National des Invalides. Ils planifient une sécurisation et un renforcement des installations techniques dont les réseaux électriques et informatiques, les systèmes de climatisation, ainsi que la densification et la rénovation des espaces de travail.

Le budget total des travaux de la programmation représente un total de 19,6 M€ (10,6 M€ pour les installations techniques, 8 M€ pour la rénovation des espaces de travail et l'entretien des bâtiments, 1 M€ pour l'aménagement d'un bâtiment de dévolution pour répondre aux besoins inhérents au plan de continuité de l'activité du SGDSN). Il est envisagé de lancer ces opérations sur les crédits du CAS Immobilier.

D'ici à l'échéance du bail du site d'implantation de l'ANSSI (1er janvier 2022), il y aura lieu d'identifier une implantation dans un nouvel immeuble qui devra répondre à la croissance de l'effectif[1], à l'élargissement des missions de l'agence et à l'accueil des moyens techniques essentiels à son fonctionnement.

III. LES FONDS SPÉCIAUX

A. UNE ENVELOPPE DE CRÉDITS STABILISÉE

Les fonds spéciaux sont consacrés au financement de diverses actions liées à la sécurité extérieure et intérieure de l'État. Ils s'élèvent à 67,4 M€ en AE et CP dans le PLF 2017[2] (67,9 M€ en PLF 2017).

Vos rapporteurs restent perplexes. De leur point de vue, dans un contexte de revalorisation substantielle des moyens humains et budgétaires accordés aux services de renseignement, notamment en réponse à la menace terroriste, et de l'accent mis par la Revue stratégique de défense et de sécurité nationale sur la fonction de « connaissance et anticipation » et les capacités des service de renseignement, la revalorisation du montant de ces fonds opérés en 2017[3] aurait dû se poursuivre, l'exercice précédent de « sincérisation » ne constituant qu'une partielle remise à niveau.

Telle était d'ailleurs la recommandation formulée par le Commission de vérification des fonds spéciaux (CVFS) dans son rapport public annexé au rapport annuel de la Délégation parlementaire au renseignement (DPR) pour 2016[4]. « *La CVFS continue à plaider en faveur d'une augmentation substantielle du montant de ces crédits. Une telle évolution apparaîtrait cohérente avec l'activité opérationnelle soutenue à laquelle sont aujourd'hui confrontés les services de renseignement et permettrait également de limiter le recours à l'octroi de ressources additionnelles en cours d'année (…) en particulier par la voie de DDAI[5] », dispositif conçu pour le financement d'activités ponctuelles n'ayant pas vocation à s'inscrire dans la durée* ».

---

[1] *Il conviendra à cet égard, de considérer qu'un cadre de travail adapté est un facteur puissant d'attractivité pour les ingénieurs informaticiens.*

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

[3] *En 2016 le montant inscrits au PLF était de 47,3 M€.*

[4] *Rapport de la délégation parlementaire au renseignement pour 2016 http://www.senat.fr/rap/r16-448/r16-448.html p.85*

[5] *Décrets pour dépenses accidentelles et imprévisibles.*

B. LE CONTRÔLE DE L'UTILISATION DES FONDS SPÉCIAUX

Le contrôle de l'utilisation des fonds spéciaux a été confié par le législateur (article 154 de la loi de finances pour 2002) à la CVFS[1]. Ces travaux sont couverts par le secret de la défense nationale[2]. La CVFS constitue une **formation spécialisée au sein de la DPR.** Depuis 2016, elle publie un rapport public en annexe de celui de cette Délégation.

[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.*

[2] *Les vérifications terminées, la commission établit un rapport sur les conditions d'emploi des crédits. Le rapport est présenté aux membres de la délégation parlementaire au renseignement qui ne sont pas membres de la commission. Il est également remis, par le président de la délégation, aux présidents et rapporteurs généraux des commissions de l'Assemblée nationale et du Sénat chargées des finances ainsi qu'au Président de la République et au Premier ministre.*

La commission dresse un procès-verbal dans lequel elle constate que les dépenses réalisées sur les crédits visés au I sont couvertes par des pièces justificatives pour un montant égal. Le procès-verbal est remis par le président de la commission au Premier ministre et au ministre chargé du budget qui le transmet à la Cour des comptes.

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).

Leur activité s'est élargie ces dernières années pour s'adapter à des besoins croissants de formation et d'information sur les politiques de défense et de sécurité nationale. Cet accroissement d'activité s'est inscrit au cours des derniers exercices dans un contexte de réduction des subventions pour charges de service public (SCSP) et des emplois.

Pour 2018, les subventions pour charges de service public et plafonds d'emploi des deux instituts sont maintenues au niveau de la LFI 2017 :

- pour IHEDN à 7,6 M€ en AE et en CP et 92 ETPT ;

- pour INHESJ à 6,2 M€ en AE et en CP et 73 ETPT.

I. L'INSTITUT DES HAUTES ÉTUDES DE DÉFENSE NATIONALE

A. MISSIONS ET ACTIVITÉS DE L'IHEDN

L'IHEDN a pour mission de développer l'esprit de défense et de sensibiliser aux questions internationales. Il organise des sessions de formation destinées aux responsables de haut niveau de fonction publique civile et militaire ainsi qu'aux différentes catégories socio-professionnelles de la Nation, des États membres de l'UE ou d'autres États.

1. Un plan stratégique qui tarde à se matérialiser en l'absence de contrat d'objectifs et de performance

Les orientations stratégiques ont été formalisées dans un Plan Stratégique IHEDN 2020[1] adopté en novembre 2015

Pour autant, l'IHEDN et sa tutelle n'ont pas réussi, deux ans après son adoption, à mettre en place un contrat d'objectifs et de performance comme nombre d'établissements publics. Selon les informations recueillies, le projet ne sera pas soumis au conseil d'administration d'ici la fin de l'année. L'existence d'un tableau de suivi de la mise en œuvre des orientations du plan stratégique ne peut en tenir lieu.

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

Dans son rapport pour avis sur le PLF 2017, votre Commission avait observé que ces retards induisent un décalage temporel entre la définition de la stratégie et la matérialisation du soutien de l'autorité de tutelle. Vos rapporteurs réitèrent cette observation. Ces retards laissent supposer l'existence de dysfonctionnements soit dans le fonctionnement administratif de l'Institut, soit dans l'exercice du pilotage des relations avec l'Etat. **Vos rapporteurs demandent que le SGDSN exerce son autorité de tutelle avec fermeté pour sortir de cette inertie.**

2. Les activités de l'IHEDN

Selon le rapport d'activité de l'institut, l'année 2016 a vu un accroissement minime du nombre de journées de formation/auditeurs-participants qui passe de 26 334 en 2015 à 26 593 soit un peu moins de 1%. Les formations stricto sensu représentent près de 90% de l'activité. Les formations au niveau national constituent 80% de l'activité : les sessions nationales (*politique de défense, armement et économie de défense, enjeux maritimes*) un peu plus de 40% (39,5% en 2015), les séminaires jeunes près de 15% et les sessions en région près de 17% (18% en 2015).

Au niveau national, la création d'une session « *Enjeux et stratégies maritimes* » connaît un certain succès. En revanche, les sessions « jeunes » et en région progressent peu. Un effort a été produit sur les journées d'information. L'année 2017 s'est inscrite dans la continuité de 2016 avec la reconduction des activités de formation et d'information[1].

La mutualisation avec l'INHESJ initiée en 2011 s'est poursuivie[2].

Si le rapport d'activité de l'IHEDN[3] 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 activité, 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 et présente *a minima* des données équivalentes à celles exposées dans le rapport annuel de l'INHESJ (indicateurs détaillés de satisfaction des auditeurs et stagiaires, nombre de personnes formées et nombre d'heures/stagiaires par département).

---

[1] *Les réponses au questionnaire budgétaire font apparaître pour 2017 des volumes horaires, ce qui laisse présager une évolution du mode de présentation dans les prochains rapports d'activités, mais à défaut de disposer des volumes horaires des précédentes années, il est impossible de mesurer quantitativement l'activité de l'Institut.*

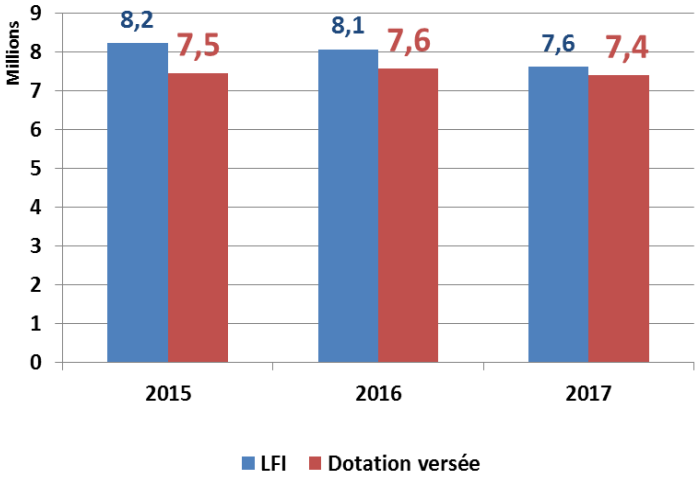
[2] *voir infra p.74*

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

Vos rapporteurs constatent que les rapports annuels continuent à présenter des statistiques par journée et ne mettent pas en rapport ces éléments « physiques » avec les données comptables.

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.



Source : SGDSN – réponse au questionnaire parlementaire

Les effectifs de l'IHEDN ont été réduits de 12 ETP entre 2014 et 2017 et la subvention pour charges de service public a été réduite de 8,8 M€ en 2012 à 7,4 M€ en 2017, soit une baisse de 16,4%. Pour autant, le budget global est resté stable, autour de 10 M€ grâce à une augmentation constante des recettes propres qui atteignent 2,8 M€ en 2017.

En 2016 la part des subventions représente 77,4% des produits (sensiblement comme en 2015) alors qu'elle atteignait respectivement 78% en 2014 et 81% en 2013. La part des ventes de prestations continue à augmenter : 14% en 2013, 18% en 2014, 19% en 2015 et 21,6% en 2016.

Le montant de la subvention annoncée pour 2017 après régulation est de 7,4 M€. L'IHEDN supporte une diminution de l'ordre de 2% de ses crédits de fonctionnement par rapport à 2016 ; en outre, deux emplois ont été supprimés, le nombre d'ETPT autorisé revenant à 92[1].

---

[1] *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*.

L'IHEDN bénéficie en outre du soutien logistique du ministère de la défense pour l'organisation, notamment, de déplacements et de présentations, ce qui est indispensable à son fonctionnement et à la qualité des formations qu'il dispense.

L'équation budgétaire est demeurée sous tension même si l'écart entre les recettes attendues et les recettes réalisées s'est avéré moindre qu'au cours des exercices précédents. L'IHEDN reste contraint de faire progresser ses **recettes extérieures** (droits d'inscription, partenariats, mécénats, taxe d'apprentissage) et faire preuve de **maîtrise de ses dépenses**. L'exécution budgétaire 2017 de l'IHEDN devrait atteindre une phase de stabilisation qui va renforcer la gouvernance et la trajectoire financière de l'établissement, en répondant aux exigences de sincérité et de soutenabilité.

L'exercice 2018 en maintenant subvention et plafond d'emploi au niveau de 2017 représente une opportunité de stabilisation dans la gestion de l'institut.

L'IHEDN devra poursuivre une mutation dans son organisation pour transformer sa structure d'emploi et l'adapter à ses nouvelles orientations stratégiques. Il pourrait ainsi poursuivre la politique de « dépyramidage » afin de recruter des emplois au plus près du cœur de métier de jeunes experts et autres spécialistes.

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. Enfin, ils réitèrent la demande de votre commission que les projets de COP soient transmis pour avis aux commissions parlementaires compétentes.

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

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. Il prépare 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[1].

[1] *Les travaux de l'ONDRP réalisés avec l'appui de l'INSEE, font l'objet de plusieurs publications dont un rapport annuel sur la criminalité en France.*

A. MISSIONS ET ACTIVITÉS DE L'INHESJ

1. Les missions formalisées dans un plan stratégique

Le plan stratégique de l'INHESJ 2015-2017[1] porte l'ambition de l'institut d'être l'opérateur de référence dans ses missions fondatrices. Ces orientations seront approfondies par un nouveau plan stratégique 2018-2021, qui devrait être approuvé d'ici la fin de l'année.

Présentation plan stratégique 2018-2020

Grâce à une réorganisation des activités de formation et de recherche de l'institut, ce plan stratégique amplifie les objectifs du plan précédent et tend vers un renforcement de la fonction prospective. Il est le socle de la construction de trois continuums :

Continuum défense/sécurité/justice

La globalisation de la menace justifie pleinement l'approche interministérielle, marque de l'institut depuis 2010. Il s'agit d'affirmer la nécessité pour un Etat de disposer d'un lieu où se construit un diagnostic partagé, apaisé et éclairé de l'état de la menace. Il s'agit ensuite d'organiser une stratégie en réponse à cette menace, dans laquelle le droit et la dimension judiciaire doivent occuper une place centrale.

Continuum recherche/action

La complexité et l'intensité des enjeux de sécurité nécessitent de recourir à des recherches scientifiques qu'il faut désormais articuler avec les exigences opérationnelles. Face à l'intensité des menaces, la dichotomie chercheurs/acteurs opérationnels est surmontée à l'institut. Dans le cas de la radicalisation, la complexité des parcours individuels et des mécanismes sociologiques, anthropologiques ou politiques, obligent à une réflexion savante avant de pouvoir tracer les axes d'une politique publique et décliner des stratégies et des programmes de prises en charge des publics concernés.

Continuum échelon central/échelon local

La nature des menaces et des risques exige une cohérence accrue entre le niveau central et le niveau local de l'action publique. La compréhension comme la détection des risques et des menaces supposent d'associer l'ensemble des acteurs, privés et publics, sur tout le territoire national. La gestion de crise, l'intelligence économique, la protection de nos concitoyens, de nos entreprises, la prévention et la lutte contre la délinquance, ne peuvent se faire que dans l'action collective. La fiabilité et l'exhaustivité des diagnostics passent par la capacité de l'Etat central à associer tous les acteurs institutionnels à la conception des politiques de sécurité et à leur mise en œuvre.

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. Il reprend les objectifs

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

stratégiques et les complète par des objectifs intermédiaires et par des indicateurs[1]. Il intègre les objectifs partagés de mutualisation avec l'IHEDN.

Un contrat d'objectifs et de performance entre l'INHESJ et l'Etat destiné à traduire les orientations du nouveau Plan stratégique sera présenté au conseil d'administration en même temps que ce dernier.

Vos rapporteurs saluent cette initiative qui répond aux observations formulées par la Commission dans son précédent rapport[2] de conduire concomitamment les deux démarches, ce qui permet aux établissements publics d'être en ordre de marche pour la période considérée, en disposant de leurs objectifs et des moyens de les évaluer.

Ils regrettent cependant que le choix ait été fait de maintenir une période de trois ans qui leur apparaît courte pour programmer le développement de cet établissement. Enfin, ils réitèrent la demande de votre Commission que les projets de COP soient transmis pour avis aux commissions parlementaires compétentes.

3. Les activités de formation et de recherche

Dans son rapport annuel, l'INHESJ publie un nombre important d'indicateurs qui permettent de mesurer son activité, d'un point de vue quantitatif et qualitatif.

a) Les activités de formation

En 2016, l'INHESJ a délivré 2 297 heures de formation (1 969 en 2015 et 1 928 en 2014) au profit de 1 719 auditeurs et stagiaires (1 631 en 2015 et 1 754 en 2014). Il publie dans son rapport annuel le nombre d'heures stagiaires qui constitue le critère habituel d'évaluation dans le secteur de la formation pour mesurer l'activité et s'établit en 2016 à 68 456 et pour 7 574 journées stagiaires (indicateur utile pour suivre l'utilisation des locaux).

D'un point de vue qualitatif l'indicateur de satisfaction des auditeurs et stagiaires a sensiblement progressé en 2016. La moyenne des 3 sessions nationales passant de 3,08 à 3,49/4[3], alors que les indicateurs concernant les autres cycles se maintiennent.

Les différents départements ont été incités à développer l'offre de formation afin d'augmenter les ressources propres de l'établissement,

---

[1] *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*

[2] *Sénat - Projet de loi de finances pour 2017 Avis n° 142 (2016-2017) du 24 novembre 2016, Tome IX - par MM. Jean-Marie Bockel et Jean-Pierre Masseret p.90*

[3] *Nette progression pour la session « protection des entreprises et intelligence économique et pour la session « management stratégique de la crise, légère dégradation pour la session « Sécurité et justice ». Légère progression pour les cycles organisés par le département Intelligence et sécurité économique et petite érosion pour les sessions organisées par le département 3risques et crises ».*

notamment en répondant à des appels d'offre publics. Les formations représentent environ 80% des ressources propres. Une de ses caractéristiques est de délivrer des formations diplômantes.

Le département formation « sécurité-justice » assure principalement la mise en œuvre de la session nationale « Sécurité et Justice » et des cycles régionaux destinés aux étudiants de Master II et aux jeunes actifs. Des formations spécifiques sont également proposées. Il est le principal département avec plus de 50% des heures/stagiaires délivrées (35 287), mais un nombre de stagiaires limités (326).

Le département « intelligence et sécurité économiques » propose une gamme étendue de formations allant d'une session nationale diplômante inscrite au répertoire national des certifications professionnelles (RNCP) qu'il délivre à un nombre restreint de personnes (119) pour 15 528 heures/stagiaires délivrées.

Le département « risques et crises » dispense des formations de haut niveau destinées aux décideurs et aux cadres en charge des politiques de gestion des risques et des crises. Il a pour objectif de faire inscrire sa session nationale spécialisée au RNCP. Il dispose d'une forte expérience pédagogique et d'outils de qualité, comme le plateau de gestion de crise. Le département accompagne le SGDSN dans la rédaction du scénario technique d'exercices majeurs pour la cellule interministérielle de crise et le ministère de l'intérieur dans une réflexion sur l'anticipation. Le département conduit également des diagnostics de dispositifs de gestion de crise pour le compte de ministères et d'opérateurs de l'Etat. Les formations sont plus courtes, le nombre de stagiaires plus nombreux (1 264) et le nombre d'heures/stagiaires (17 731) représente un peu plus du quart de l'ensemble.

b) Les activités d'études et recherches

Le département « études et recherches » a mené plusieurs travaux de recherche en 2017 et en a proposé de nouveaux s'étalant jusqu'en 2019 sur l'analyse de certains risques et menaces.

Par ailleurs, l'INHESJ assure le secrétariat général du Conseil scientifique sur les processus de radicalisation[1].

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 son équipe de chercheurs, répond lui-même régulièrement à des appels à projets ou commandes publiques, et recherche des financements extérieurs pour consolider ses propres projets[2]. Les études et recherches représentent près de 20% des ressources propres.

c) Les infrastructures

Sur le plan immobilier, l'institut a déménagé en février 2016 dans une partie du bâtiment 13 de l'École militaire entièrement rénové. Ce

---

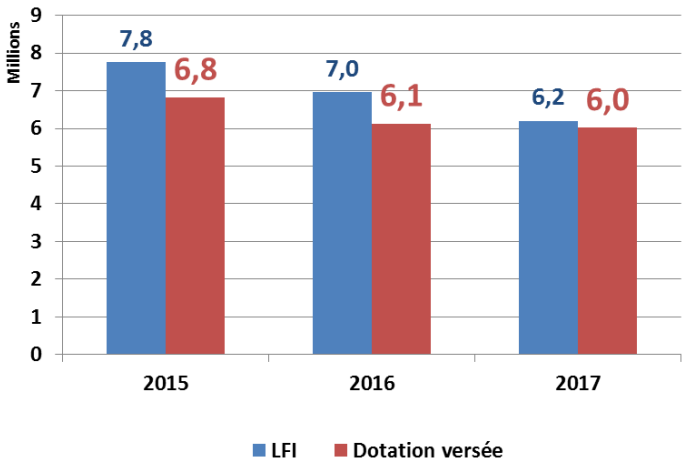
[1] *Créé par décret n° 2017-693 du 3 mai 2017, le Conseil est chargé de faciliter le dialogue entre les administrations publiques et les chercheurs en sciences humaines et sociales, et de contribuer à la valorisation des résultats de la recherche et à leur réutilisation au bénéfice des politiques publiques de prévention et de lutte contre la radicalisation*

[2] *Des démarches en ce sens sont par exemple engagées auprès de l'Agence nationale de la recherche, la Mission interministérielle de lutte contre les drogues et les conduites addictives (MILDECA), le Centre de recherche et de formation à la recherche stratégique et la Commission européenne, etc.*

bâtiment héberge un nouveau plateau de formation à la gestion de crise équipé des technologies de pointe en la matière.

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

1. Une subvention pour charges de service public en voie de stabilisation



Source : SGDSN – réponse au questionnaire parlementaire

La subvention **pour charges de service public de l'INHESJ** a été réduite de 0,8 M€ de 2015 à 2017 (1,6 en PLF).

En outre, des annulations de crédits ont été appliquées aux subventions à hauteur de 0,8 M€ en 2016, cette dernière annulation étant par ailleurs « soclée » dans le budget 2017, ce qui n'a pas facilité la gestion[1].

Ces baisses ont pu être compensées par une hausse des ressources propres, des économies de gestion et la mutualisation de certaines fonctions supports avec l'IHEDN (voir infra p. 74).

Pour 2018, la subvention pour charges de service public s'élève à 6,2 M€ en AE et en CP, soit le même montant qu'en PLF 2017, ce qui devrait constituer un socle pour son développement.

Le SGDSN abondera l'INHESJ d'un complément de subvention de 70 k€ en 2018 pour lui permettre d'assurer le secrétariat général Conseil scientifique sur les processus de radicalisation (voir supra p.71).

---

[1] *Sénat - Projet de loi de finances pour 2017 Avis n° 142 (2016-2017) du 24 novembre 2016, Tome IX - par MM. Jean-Marie Bockel et Jean-Pierre Masseret p.92*

2. Des ressources propres en progression

Les ressources sont complétées par le produit des différentes formations et études réalisées par l'établissement, plus marginalement des produits des publications et de la perception de la taxe d'apprentissage. La baisse de la subvention a pu être compensée en 2017 par une hausse de 8% des ressources propres, lesquelles atteignent 1,6 M€.

3. Des effectifs plafonnés

Les effectifs ont été réduits de 8 ETP entre 2014 et 2017. L'INHESJ a également procédé à un « dépyramidage » des postes, ce qui a permis de diminuer sensiblement sa masse salariale[1], par des recrutements ciblés et moins coûteux (jeunes chercheurs spécialisés, par exemple).

Pour 2017, le plafond d'emplois est maintenu au même niveau de 73 ETPT[2]. **A cet égard, vos rapporteurs observent une certaine contradiction entre l'exigence donnée à l'INHESJ de développer ses ressources propres en engageant de nouvelles formations et recherches, pour lesquelles il est légitime et qui sont économiquement rentables, au besoin en répondant à des appels d'offres, d'une part, et le plafonnement de l'effectif de ses personnels qui ne permet guère de lancer la préparation et la réalisation de ces actions. Le déplafonnement assurerait la pérennité du modèle économique sans solliciter d'augmentation de la subvention pour charges de service public.**

4. Une politique de maîtrise des dépenses publiques

La situation immobilière se limite, à compter de 2017, à l'occupation d'une partie du bâtiment 13 de l'École militaire. Une convention de financement des travaux de réhabilitation, signée en 2015, prévoit que le ministère des armées met des locaux à disposition de l'INHESJ en contrepartie d'une participation au financement de la réhabilitation. Cette dépense est prise en charge par le SGDSN directement[3].

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

---

[1] *Celle-ci est passé de 5,79 M€ en 2013 à 4,89 en 2016*

[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 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.*

[3] *Une mesure d'économie pourra être réalisée à la fin de l'amortissement financier du bâtiment en 2020, à hauteur de 1,8 M€[3]. La convention de financement arrête en effet le montant définitif de la contribution financière et l'échéancier de règlement (contribution du SGDSN fixée à 60% du montant total, en fonction des surfaces occupées). Entre 2016 et 2019 inclus, la contribution du SGDSN est celle d'une annuité constante de 1,8 M€, versée au ministère des armées.*

activités et du fonctionnement. L'Institut envisage de mieux structurer son contrôle de gestion, grâce à la mise en place d'une comptabilité analytique[1].

Vos rapporteurs se réjouissent des progrès réalisés au cours des dernières années par l'INHESJ pour donner plus de cohérence à sa gestion, ce qui facilitera le pilotage de la mise en œuvre du plan stratégique et des objectifs du COP. Il devra à l'avenir, pour dégager des marges de manœuvre, développer ses ressources propres, poursuivre sa politique de réduction des coûts de fonctionnement, notamment par le rapprochement et la mutualisation engagés avec l'IHEDN, et assurer une gestion plus dynamique de son personnel pour répondre aux nouveaux besoins de formation dans ses domaines de compétence.

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

Depuis 2011, **l'IHEDN et l'INHESJ sont engagés dans un processus de rapprochement qui se matérialise 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.

Les personnels mis à disposition par chaque établissement ont été regroupés.

L'harmonisation et la dématérialisation des procédures administratives, financières et comptables constituent un chantier à moyen terme.

Enfin, l'IHEDN a déployé un nouveau système d'information financière, dans le cadre du décret relatif à la nouvelle gestion budgétaire et comptable publique (GBCP) qui impose une nouvelle organisation pour optimiser le traitement et la maîtrise de la dépense publique[2]. De nombreuses difficultés ont été rencontrées liées principalement à un outil informatique techniquement peu fiable.

Cette orientation est un des points de rapprochement et de collaboration entre l'IHEDN, pilote, et l'INHESJ. Les convergences méthodologiques résultent du partage

---

[1] *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.*

[2] *Retenu parmi les 50 organismes pilotes, l'IHEDN a basculé depuis le 1er janvier 2016 dans le nouvel environnement financier. L'application de la réforme financière instaure une comptabilité budgétaire distincte de la comptabilité générale, mais avant tout, de nouvelles organisations visant à optimiser le traitement et la maitrise de la dépense publique.*

d'expérience organisé à compter de 2017. Dès lors que les outils GBCP seront stabilisés, la démarche d'harmonisation et de dématérialisation devrait pouvoir être conduite.

- 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.

Si le rapprochement se poursuit en matière informatique, il a peu avancé dans le domaine, évidemment plus sensible, du pilotage des ressources humaines.

Au-delà de ces objectifs somme toute modestes, la mutualisation 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. Il est probable que des efforts plus marqués seront attendus sur ce point notamment lorsque sont abordés certaines questions manifestant le continuum entre défense, sécurité nationale et sécurité intérieure[1].

Ce rapprochement des fonctions supports et la concertation sur l'offre de programmes restera l'un des axes des plans stratégiques et des contrats de performance à venir.

Cependant, vos rapporteurs estiment que pour progresser efficacement sur cet axe, il serait souhaitable de faire converger davantage les démarches stratégiques et contractuelles des deux Instituts. Il serait souhaitable que les plans stratégiques et les COP portent sur la même période et que les dirigeants de chacun des deux Instituts associent leurs homologues respectifs à la démarche conduite au sein de leur établissement. Il est dommage que cette recommandation de votre Commission dans son avis sur le PLF 2017 n'ait pas été encore engagée de façon explicite.

A minima, vos rapporteurs souhaiteraient que les deux établissements disposent des mêmes indicateurs d'activités et de performances pour permettre l'évaluation de la mise en œuvre de leur COP respectif **et que ces indicateurs figurent en annexe de leur rapport annuel d'activités**[2].

---

[1] *terrorisme, continuum menaces extérieures-internes, cohésion nationale-défense-citoyenneté-valeurs républicaines, cybersécurité-cyberdéfense, emploi des militaires sur le territoire, migrations et géopolitique, judiciarisation des conflits, etc…*

[2] *Les éléments figurant dans le rapport annuel de l'INHESJ constituent une base minimale utile. Vos rapporteurs engagent l'IHEDN à la reprendre dès 2017.*

EXAMEN EN COMMISSION

La commission, sous la présidence de M. Christian Cambon, président, a examiné le présent rapport pour avis lors de sa réunion du 8 novembre 2017.

M. Christian Cambon, président. - Nous ouvrons l'examen des avis de la commission sur le projet de loi de finances pour 2018, par celui portant sur le programme 129 « Coordination du travail gouvernemental ».

M. Rachel Mazuir, co-rapporteur pour avis. - Cette action, qui représente plus de la moitié des crédits de ce programme, recouvre, pour l'essentiel, les crédits du Secrétariat général de la défense et de la sécurité nationale dont ceux de l'Agence nationale de sécurité des systèmes d'information (ANSSI), ceux du GIC (Groupement interministériel de contrôle), les fonds spéciaux et les subventions destinées à deux établissements publics de formation, l'Institut des hautes études de défense et de sécurité nationale (IHEDN) et l'Institut national des hautes études de sécurité et de justice (INHESJ).

Dans un budget marqué par la volonté de réduire la dépense publique, cette action, il faut le souligner, progresse. Elle est dotée de 352 millions d'euros en AE (+1%) et de près de 354 en CP (+3%). C'est pour l'essentiel la conséquence de la poursuite de la montée en puissance du GIC pour la mise en œuvre de la loi de 2015 relative au renseignement et celle de l'ANSSI, dont vous parlera Olivier Cadic.

Je vous présenterai, pour ma part, les crédits affectés aux autres entités.

S'agissant du cœur historique du SGDSN, M. Gautier vous a exposé, le 11 octobre, la diversité de ses missions. Je voudrais formuler deux observations :

Nous constatons un développement des missions et une intensification de l'activité. L'aggravation des menaces a donc des conséquences. Pour illustrer mon propos, je relève que le rythme des réunions du conseil de défense et de sécurité nationale, s'est encore intensifié (40 réunions depuis le début de 2017). Deuxième exemple : la poursuite des déclinaisons du plan VIGIPIRATE rénové, en décembre 2016, avec l'adoption en 2017 des plans PIRANET et PIRATEMER et la préparation d'un plan METROPIRATE.

D'autre part, le SGDSN devient la structure de portage d'un ensemble d'entités plus ou moins autonomes comme l'ANSSI, le Centre des transmissions gouvernementales ou le GIC. Ensemble qui, tant en crédits qu'en effectifs, dépasse largement le cœur historique du SGDSN.

Si ces entités rattachées ont vu leurs moyens croître, tel n'a pas été le cas depuis plusieurs années du SGDSN qui a perdu 25 emplois depuis 2009 avec, pour conséquence, un affaiblissement de la fonction « Soutien » dont les effectifs représentaient 15% du total et ne représentent aujourd'hui qu'un peu plus de 7%. Votre commission avait fait cette observation l'année dernière.

Les effectifs du SGDSN stricto sensu sont maintenus dans le projet de loi de finances pour 2018, mais les crédits hors titre 2 (8,3 M€ contre 11 M€ en 2017) subissent une baisse importante. Sans doute, le budget des deux directions (« Protection et sécurité de l'État, affaires internationales et technologiques ») sera-t-il, selon le SGDSN, maintenu « à un niveau permettant son intervention dans l'ensemble des actions interministérielles concernées », mais il exigera un effort d'économies de fonctionnement et de productivité important dans un contexte de menace élevée.

Ma seconde série d'observations concerne le GIC.

La loi relative au renseignement de juillet 2015 a modifié sensiblement ses missions. Il est 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 Commission nationale de contrôle des techniques de renseignement (CNCTR).

La place du renseignement dans la lutte contre le terrorisme entraîne dans le même temps une intensification de son activité comme l'a montré le dernier rapport de la CNCTR.

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

Le rattachement effectif de son personnel au service du Premier ministre est effectif depuis l'année dernière. Au total, le GIC disposera fin 2017 de 200 ETP. Le plafond est porté à 215 en 2018 et à l'horizon 2020, il devrait employer 234 personnes. Cette perspective a été réévaluée en cours d'année 2017 en raison des prévisions d'activités. Il faut s'en féliciter. En conséquence, le titre 2 est porté à 12,6 M€.

Un effort budgétaire a été réalisé pour accompagner sa montée en puissance. Les crédits hors titre 2 sont élevés à 16,6 millions d'euros en 2017. Pour 2018, il est prévu de stabiliser cette enveloppe à 15,6 M€ réparti aux ¾ pour les crédits d'investissement et pour ¼ en fonctionnement.

Comme l'a rappelé la Délégation parlementaire au renseignement dans ses deux derniers rapports publiés, et votre commission, l'année dernière, la montée en puissance du GIC constitue le point sensible pour la mise en œuvre efficace de la loi relative au renseignement. Nous approuvons en conséquence le renforcement de son autonomie et son financement. Les modalités techniques de son adossement au SGDSN ont été précisées au

cours de l'exercice 2017, dans un projet de convention dont la signature est imminente.

Quelques mots sur les fonds spéciaux. L'enveloppe a été portée à 67,8 millions d'euros en 2017 pour accompagner la montée en puissance des services de renseignement dans la lutte anti-terroriste. C'était une recommandation de la Commission parlementaire de vérification des fonds spéciaux. La dotation baisse légèrement à 67,4 M€. C'est regrettable pour deux raisons, au-delà du symbole envoyé aux services très sollicités dans le cadre de la lutte contre le terrorisme, cela crée de l'incertitude sur la capacité d'engagement d'opérations et cela risque d'obliger le Gouvernement à compléter la dotation en cours d'année, pour financer des dépenses prévisibles, comme il avait pris l'habitude de le faire, ce qui avait été critiqué par la CVFS.

Enfin, j'en viens aux deux opérateurs l'IHEDN et l'INHESJ. L'un et l'autre achèvent leur restructuration. L'exercice 2018 constitue une respiration dans la mesure où pour la première fois depuis longtemps les crédits et les plafonds d'emplois sont reconduits. Les établissements sont invités à développer leurs ressources propres. Pour ce faire, il serait utile d'apporter de la souplesse en matière de gestion des effectifs surtout lorsqu'il s'agit de recruter pour mettre en place des formations qui apportent des ressources nouvelles. Les deux instituts sont engagés dans de nouvelles démarches de négociation d'un plan stratégique pour l'INHESJ et de formalisation d'un contrat de performance pour l'IHEDN. Si la mutualisation des capacités entre les deux instituts engagée depuis 2011 se concrétise sur le plan du soutien, elle reste à conforter pour l'offre de programmes dans les domaines comme l'intelligence économique ou le continuum sécurité/défense. À nos yeux, cette démarche mériterait d'être consolidée au niveau stratégique par l'implication croisée des deux directeurs dans l'élaboration des plans stratégiques et contrats de performance respectifs.

M. Olivier Cadic, co-rapporteur pour avis. - Je m'associe aux propos de Rachel Mazuir et formulerai pour ma part quelques observations concernant l'ANSSI.

La cyberdéfense est un enjeu majeur. Dans une société de plus en plus connectée, les systèmes d'information sont des points de vulnérabilité. Assurer la protection contre une cybercriminalité puissante et virulente, mais aussi face au développement de l'espionnage et désormais, des actions d'ingérence de puissances étrangères, comme on a pu l'observer lors des campagnes électorales américaines et françaises, est devenu un impératif. Selon le rapport « Symantec 2017 », la France est passée au 8ème rang des pays où la cybercriminalité est la plus active et au 4ème rang en Europe. Le rapport observe une recrudescence des e-mails contenant des pièces jointes malveillantes. Un mail sur 131 est malveillant dans le monde contre 220 en 2015. Le rapport enregistre une hausse de 36 % du nombre de rançongiciels et en a identifié plus de 100 nouvelles familles. Cette activité se révèle

toujours plus lucrative ; la rançon moyenne est passée en un an de 294 à 1 077 $. Ce type d'attaques n'a pas progressé en France sans doute parce que seules 30% des victimes paient les rançons contre 64% aux États-Unis. En mai 2017, l'attaque massive à base de logiciels malveillants, exploitant une faille de Windows, a touché plus de 100 000 systèmes dans près de 100 pays dont ceux d'un certain nombre de grandes entreprises, en France et à l'étranger, ainsi que le service de santé britannique. Notre pays n'est pas épargné par les vols d'identifiants. Avec 85,3 millions d'identifiants volés, elle pointe à la 2ème place mondiale. Enfin, 2016 a connu la plus grande attaque par déni de service distribuée exploitant des réseaux d'objets connectés marquant l'émergence fulgurante de ce risque. Au plus fort de cette action massive, on enregistrait des attaques toutes les 2 minutes.

Face à cette menace croissante, l'ANSSI met en œuvre la stratégie nationale de sécurité informatique. Elle a développé toute une série d'activités à partir de ses laboratoires d'expertise. Son périmètre d'action s'est élargi au-delà de la protection des administrations de l'État. Les textes d'applications de la LPM de décembre 2013 concernant les opérateurs d'importance vitale sont désormais publiés. Elle investit dans la mise au point de certains produits de sécurité. Elle en labélise d'autres, mais aussi des prestataires de confiance et des filières de formation. Elle apporte du conseil aux services déconcentrés de l'Etat, aux collectivités territoriales et aux entreprises grâce au déploiement d'un réseau en région. Enfin, elle a participé à la création de la plateforme cybermalveillance.gouv.fr, ouverte le 17 octobre, qui met en relation particuliers et administrations locales avec des spécialistes susceptibles de leur venir en aide.

Pour autant, un point de faiblesse demeure. Trois ans après la publication de la Politique de sécurité des systèmes d'information de l'Etat (PSSIE), le retard, au regard des objectifs de conformité affichés peine à être comblé. L'insuffisance des moyens consacrés à la sécurité dans les ministères ainsi que des contraintes techniques et d'organisation qui ne permettent pas toujours à l'ANSSI de déployer des sondes dans des conditions adaptées à la menace, ni de recueillir toutes les informations nécessaires pour assurer une détection optimale, explique cela. Les ministères régaliens sont les bons élèves, mais quand on voit les attaques se développer comme en Grande-Bretagne en mai dernier, contre les services de santé, on peut légitimement être inquiet. Ce point avait déjà été relevé l'année dernière.

Il nous semble nécessaire qu'une inspection identifie les difficultés et propose un plan d'action et que soient étudiés rapidement les moyens permettant à l'ANSSI d'imposer ses préconisations aux directions des systèmes d'information des ministères.

La politique de cyberdéfense connaîtra sans doute en 2018 de nouveaux développements. Une revue est conduite par le SGDSN, et vous aurez également remarqué la présence accentuée du cyber dans la revue

stratégique de défense qu'est venue nous présenter Arnaud Danjean récemment.

Pour ce faire, l'ANSSI voit ses moyens progresser en 2018.

Ses effectifs passeront de 547 à 572 ETP, +25. L'Agence considère toutefois que son effectif devrait être d'une centaine d'agents supplémentaires. Au vu des perspectives actuelles, à raison de 25 ETP par an, cette cible ne devrait être atteinte qu'en 2022. C'est pour nous un facteur de préoccupation, compte tenu de l'évolution des menaces. Espérons que la revue de cyberdéfense sera un levier en faveur d'une montée en puissance plus rapide. Les problèmes de recrutement et de fidélisation des cadres sont en voie de solution progressive, mais la vigilance demeure car les spécialistes de la sécurité informatique continueront à être très recherchés, tant dans le secteur public que dans le secteur privé.

La faiblesse du vivier demeure inquiétante. L'engagement de l'ANSSI dans une politique de labélisation des formations est positif, mais il devrait 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 et à diffuser dans toutes les filières la culture de la cybersécurité qui est désormais, soyons-en conscients, un enjeu majeur de société.

Les crédits affectés à l'ANSSI sont compris dans le budget du SGDSN, ce qui ne permet pas une lecture aisée des documents budgétaires. Il serait souhaitable, ce sera une de nos recommandations, de les faire apparaître indépendamment, sous forme d'une unité opérationnelle à l'instar du GIC, qui comme l'ANSSI est un service à compétence nationale.

Ils progressent sensiblement en crédits de paiement atteignant 73,39 M€ (+11,4%) et sont stables en autorisations d'engagement (-1,1%). La principale opération d'investissement concerne le centre de stockage des données pour stocker et traiter les données recueillies lors des cyberattaques. L'investissement est porté par le ministère de l'intérieur pour un coût total de 24,2 millions d'euros, que le SGDSN finance aux trois-quarts. Les AE (18,2 millions d'euros) ont été transférées en 2016. En 2018, 6 millions sont inscrits en CP. Pour le reste, les crédits servent, pour l'essentiel, au développement de produits de sécurité pour la protection des informations classifiées, à des acquisitions de matériel informatique, au fonctionnement des systèmes d'information sécurisé, à la politique d'expertise scientifique et technique de l'Agence et à son fonctionnement opérationnel.

Globalement, nous sommes satisfaits de l'évolution des crédits de cette action et donc de ce programme 129 et vous proposons d'exprimer un avis favorable à l'adoption de la mission « Direction de l'action du gouvernement ».

M. Jean-Marie Bockel. - La menace évolue à une vitesse incroyable et il faut saluer la mobilisation croissante des autorités publiques qui ont pris

suffisamment tôt conscience de l'ampleur de cette menace et su réagir rapidement en développant les moyens nécessaires pour y faire face. Je mesure l'effort accompli, même s'il ne faut pas baisser la garde. Il me semble que nous devons maintenant développer notre action à l'international, dans des enceintes comme les Nations unies. C'est un point que nous avions esquissé dans le rapport de la mission d'information de la commission sur ce sujet en 2012. Il est souhaitable que des règles du jeu puissent être établies pour lutter contre la cybercriminalité et réguler autant que faire se peut le comportement des États dans le cyberespace. Même si elles ne sont pas toujours respectées, on sait que, à la longue, elles font peser sur les États un risque de réputation et de marginalisation auquel ils sont sensibles, même les moins démocratiques d'entre eux.

M. Ladislas Poniatowski. - Pourriez-vous nous décrire très concrètement en quoi consiste le rançonnage informatique ?

M. Olivier Cadic, co-rapporteur. - Je partage l'appréciation de Jean-Marie Bockel sur l'action à mener dans les enceintes internationales. Une agence se crée au niveau européen dans laquelle l'ANSSI est impliquée.

S'agissant du rançonnage, cela consiste, pour une organisation criminelle, à bloquer l'accès aux données qui permettent d'exploiter un système informatique, qui peut être un système de production industrielle ou de transport, comme le système d'information d'une entreprise ou d'une administration en les cryptant et en sollicitant une rançon en échange de la clef de décryptage, rançon acquittée en général en monnaie virtuelle (type bitcoin) pour empêcher la traçabilité de la transaction. Il ne s'agit pas de vols ou de destruction de données, encore que certaines attaques puissent combiner tous ces aspects.

M. Rachel Mazuir, co-rapporteur. - Ces moyens nouveaux de cyberattaque peuvent paralyser des services publics de base, dont la vulnérabilité s'est accrue avec l'introduction de systèmes informatiques à base de réseaux et d'objets connectés. On n'a pas encore tout à fait mesuré l'ampleur de ces risques et ce qui m'inquiète un peu, c'est le retard de certaines administrations à faire tous les efforts nécessaires pour s'en protéger. C'est un travail de sensibilisation que nous devons mener.

M. Christian Cambon, président. - Je voulais vous livrer une anecdote qui est celle d'un expert en sécurité informatique qui a montré, au cours d'un congrès international de médecins, comment, au moyen d'un logiciel acquis à bon marché, il était en mesure de recueillir en quelques minutes et en direct des données présentes dans les mémoires de téléphones mobiles de participants en ne connaissant que leur seule identité. Tout cela pour démontrer que ces technologies se diffusent à grande échelle.

La commission donne, à l'unanimité, un avis favorable à l'adoption des crédits de la mission « Direction de l'action du Gouvernement ».

ANNEXE –
LISTE DES AUDITIONNÉS

➢ **Audition en commission plénière :**

- Mercredi 11 octobre 2017 :

M. Louis Gautier, secrétaire général de la défense et de la sécurité nationale.

Compte-rendu consultable sur le site Internet du Sénat à l'adresse suivante :
http://www.senat.fr/compte-rendu-commissions/20171009/etr.html

➢ **Auditions par les rapporteurs :**

- Mercredi 18 octobre 2017

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

- Mardi 31 octobre 2017 :

M. Pascal Chauve, directeur du GIC