N° 149

SÉNAT

SESSION ORDINAIRE DE 2018-2019

Enregistré à la Présidence du Sénat le 22 novembre 2018

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**, ADOPTÉ PAR L'ASSEMBLÉE NATIONALE, *pour* **2019**,

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, M. Robert del Picchia, Mme Sylvie Goy-Chavent, MM. Jean-Noël Guérini, Joël Guerriau, Pierre Laurent, Cédric Perrin, Gilbert Roger, Jean-Marc Todeschini, *vice-présidents ;* M. Olivier Cigolotti, Mme Joëlle Garriaud-Maylam, M. Philippe Paul, Mme Marie-Françoise Perol-Dumont, *secrétaires ;* MM. Jean-Marie Bockel, Gilbert Bouchet, Michel Boutant, Olivier Cadic, Alain Cazabonne, Pierre Charon, Mme Hélène Conway-Mouret, MM. Édouard Courtial, René Danesi, 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, MM. Gérard Poadja, Ladislas Poniatowski, Mmes Christine Prunaud, Isabelle Raimond-Pavero, MM. Stéphane Ravier, Hugues Saury, Bruno Sido, Rachid Temal, Raymond Vall, André Vallini, Yannick Vaugrenard, Jean-Pierre Vial, Richard Yung.

Voir les numéros :

Assemblée nationale (**15**ème législ.) : **1255**, **1285**, **1288**, **1302** à **1307**, **1357** et T.A. **189**

Sénat : **146** et **147** à **153** (2018-2019)

SOMMAIRE

Pages

LES PRINCIPALES OBSERVATIONS 5

INTRODUCTION 7

TITRE PREMIER : LE SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN) ET LES ENTITÉS RELEVANT DU PROGRAMME 129 9

I. LE SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN), OUTIL INTERMINISTÉRIEL DE PRÉVENTION ET DE GESTION DES CRISES 9

II. LE SGDSN, ACTEUR DE LA POLITIQUE DE SÉCURITÉ NATIONALE 12

III. L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI), BRAS ARMÉ DE L'ÉTAT POUR LA CYBERDÉFENSE 18

A. UNE MENACE QUI NE CESSE DE S'ACCROÎTRE EN INTENSITÉ ET EN SOPHISTICATION 19

B. UNE DÉMARCHE STRATÉGIQUE ENGAGÉE POUR FAIRE FACE À CETTE MENACE 20

C. LE RENFORCEMENT DU CHAMP DES COMPÉTENCES DE L'ANSSI 20

D. UNE CAPACITÉ D'EXPERTISE DE TRÈS HAUT NIVEAU 22

E. LES ACTIONS DE L'ANSSI VERS LES ADMINISTRATIONS 22

F. L'ÉLARGISSEMENT DU PÉRIMÈTRE D'ACTION 27

G. L'ANSSI, ACTEUR DE LA CONSOLIDATION DE LA FILIÈRE FRANÇAISE DE SÉCURITÉ INFORMATIQUE 31

H. LES RELATIONS INTERNATIONALES 33

I. LE SUIVI, LE CONTRÔLE DE L'ACTIVITÉ DE L'ANSSI ET L'ÉVALUATION DE SA PERFORMANCE 35

IV. LE CENTRE DE TRANSMISSIONS GOUVERNEMENTAL (CTG) 35

V. LE GROUPEMENT INTERMINISTÉRIEL DE CONTRÔLE (GIC) 36

A. DES MISSIONS EN VOIE DE STABILISATION 36

B. LA CONSOLIDATION DE SON FORMAT ET DE SON ORGANISATION 37

TITRE 2 : LES MOYENS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2018 41

I. LES CRÉDITS DE TITRE 2 ET LA POLITIQUE DES RESSOURCES HUMAINES 42

A. LES CRÉDITS ET LES EMPLOIS INSCRITS AU BOP SGDSN 42

B. LE SGDSN : UNE VIGILANCE A GARDER SUR L'ORGANISATION DES FONCTIONS DE SOUTIEN 43

C. L'ANSSI : POURSUIVRE LA MONTÉE EN PUISSANCE EN CONSERVANT LE NIVEAU DE COMPÉTENCE ET D'EXPERTISE 43

D. LE GIC : GARDER LA MAÎTRISE DE SES EFFECTIFS ET ASSURER LEUR MONTÉE EN PUISSANCE 47

II. LES CRÉDITS DE FONCTIONNEMENT ET D'INVESTISSEMENT INSCRITS AU « BOP » SGDSN 50

A. SGDSN/ANSSI : DES ACTIONS NOMBREUSES ET DIVERSES À SOUTENIR (LES CRÉDITS HORS TITRE 2 EN PLF 2019) 50

B. LA POURSUITE DE L'EFFORT BUDGÉTAIRE POUR ACCOMPAGNER LA MONTÉE EN PUISSANCE ET L'INTENSIFICATION L'ACTIVITÉ DU GIC 54

III. LES FONDS SPÉCIAUX 57

A. LA GESTION ET LE CONTRÔLE DES FONDS SPÉCIAUX 57

B. UNE ENVELOPPE DE CRÉDITS STABILISÉE 58

TITRE 3 : LES INSTITUTS RATTACHÉS AU SGDSN 59

I. L'INSTITUT DES HAUTES ÉTUDES DE DÉFENSE NATIONALE 59

A. MISSIONS ET ACTIVITÉS DE L'IHEDN 59

B. L'ÉVOLUTION DES CRÉDITS ET DES EMPLOIS DE L'IHEDN 61

II. L'INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE 62

A. MISSIONS ET ACTIVITÉS DE L'INHESJ 62

B. L'ÉVOLUTION DES CRÉDITS ET DES EMPLOIS DE L'INHESJ 65

III. LE RAPPROCHEMENT ENGAGÉ ENTRE L'IHEDN ET L'INHESJ 67

EXAMEN EN COMMISSION 69

ANNEXE – LISTE DES AUDITIONNÉS 76

LES PRINCIPALES OBSERVATIONS

1. Au sein **programme 129 « *Coordination du travail gouvernemental*** d'un montant de 692,14 M€, (soit 52 % des CP prévus pour l'ensemble de la mission « *Direction de l'action du gouvernement* »), **les crédits sous examen de vos rapporteurs pour avis correspondent à l'action 02 « *Coordination de la sécurité et de la défense* »** dotée de **378,49 M€** en AE et de **362,13 M€** en CP. Elle enregistre une **croissance** en CP **(2,57 %, + 9,6 M€**) comme en AE **(7,7%, 27,1 M€)** par rapport à la prévision inscrite dans la loi de finances pour 2018.

Comme en 2018, l'évolution du programme 129 continue de s'inscrire dans la priorité portée par l'ANSSI de montée en puissance de la politique de sécurité des systèmes d'information et de protection contre les menaces croissantes dans le cyberespace et dans celle du GIC qui poursuit sa transformation pour accompagner l'usage croissant des nouvelles techniques de renseignement.

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 et que soit étudiée pour l'ANSSI, comme cela existe pour le GIC, la mise en place d'une unité opérationnelle.

2. **Les effectifs du SGDSN (hors ANSSI) seront réduits de 5 ETP**. Le surcroît d'activité devrait pouvoir être absorbé par des gains de productivité.

Vos rapporteurs estiment qu'il faut veiller à ce que ce rouage de la coordination interministérielle en matière de sécurité et de défense, qui en outre assure le soutien de nombreuses entités, ne doit pas être affaibli dans un contexte d'aggravation des menaces.

3. **La montée en puissance de l'ANSSI est confirmée et devra s'intensifier aux cours des prochaines années en cohérence avec la transposition de la directive européenne NIS, la LPM 2019-2025 et les orientations de la *Revue stratégique de cyberdéfense* publiée en février 2018.**

Ses effectifs devraient s'accroître de 42 ETP en 2019 pour atteindre 675 ETP en 2022. Ce nombre, addition des 25 ETP prévus par le schéma d'emplois et 17 recrutements non réalisés en 2018, recouvre une réalité plus inquiétante, celle des tensions observées sur un marché du travail très concurrentiel s'agissant des profils recherchés qui enchérit les coûts et entraîne un « rebasage » des crédits du titre 2 qui progressent de 6,3 M€ en 2019.

Le vivier de formation reste insuffisant au regard des besoins. Ce problème partagé par tous les services de l'Etat a des conséquences sur leur résilience.

Vos rapporteurs souhaitent qu'une politique active de développement de filières de formation initiale soit portée au plus haut niveau de l'Etat. C'est un enjeu de sécurité nationale.

L'ANSSI représente une part importante des crédits hors titre 2. Leur progression en AE est destinée à couvrir le renouvellement du bail de la Tour Mercure pour les besoins de l'ANSSI (15,5 M€), il est aussi prévu la mise en chantier de la rénovation du réseau gouvernemental Rimbaud (13 M€).

Vos rapporteurs demandent que soit engagée rapidement une réflexion sur la localisation de l'ANSSI à l'horizon 2022 compte tenu de l'accroissement de ses missions et de ses effectifs.

Vos rapporteurs avaient alerté sur **le retard de mise en conformité des systèmes d'information de l'État** en adéquation avec les enjeux (PPSSIE). Le diagnostic a été confirmé et approfondi par la *Revue stratégique de Cyberdéfense*.

Vos rapporteurs se réjouissent de cette prise de conscience, mais ils estiment que sans portage politique majeur permanent, sans moyens financiers significatifs et sans outils réglementaires coercitifs, il sera difficile de lutter contre une logique qui valorise la multiplication de systèmes d'information et des applications numériques permettant d'abaisser des coûts de fonctionnement ou de personnels. Ils souhaitent que l'Etat fixe aux ministères la réalisation d'un ratio d'investissement dans la cybersécurité et que l'ANSSI intervienne dans le processus de recrutement des DSI ministériels, de formation des directeurs « métiers » et que des objectifs en matière de sécurité informatique définis soient explicitement imposés dans leurs lettres de mission et pris en compte dans leur évaluation.

4. Les subventions destinées à l'Institut des hautes études de la défense nationale (IHEDN) et à l'Institut national des hautes études de la sécurité et de la justice (INHESJ) sont maintenues à hauteur de 13,8 M€, ce qui constitue un socle de développement de leurs activités, notamment celles susceptibles de produire des ressources propres. La mutualisation des moyens et le développement de synergies entre les deux établissements progressent mais restent des objectifs à parfaire.

Vos rapporteurs demandent que la nouvelle direction de l'IHEDN renouvelle sa démarche stratégique et prépare concomitamment un contrat d'objectifs et de performance avec l'Etat comme l'a fait l'INHESJ.

5. Les fonds spéciaux sont maintenus à 67,4 M€.

6. Le développement de l'usage des nouvelles techniques de renseignement par les services, notamment dans la lutte contre le terrorisme, entraîne une intensification significative de l'activité du **Groupement interministériel de contrôle (GIC)** qui **poursuit sa transformation et sa montée en puissance**.

Ses effectifs devraient atteindre 243 TP en 2020. Il est prévu la création de 15 EPT en 2019. Ses crédits hors titre 2 augmentent de 15,6 à 17,1 M€.

Ce développement est toutefois freiné par des difficultés de recrutement et par la saturation des locaux. Un projet immobilier est en cours.

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

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 2019 ; les sénateurs du groupe CRCE s'abstenant.

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	684,47	692,14	1 226
ACTION 2	378,49	362,13	2 964
RATIO ACTION2/P129	55,30%	52,32%	41,37%

Sources : PLF2019

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 2019 de **378,49 M€** en autorisations d'engagement (AE) et **362,13 M€** de crédits de paiement (CP).

Ces crédits progressent de 7,7% en AE et de 2,6% en CP

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

		Titre 2	Hors titre 2	**Total**
Autorisations d'engagement	2019	97 206 797	281 285 961	**378 492 758**
	2018	89 674 675	261 671 743	**351 346 418**
	2017	80 513 246	167 781 197	**248 294 443**
	2016	66 377 128	151 094 926	**213 472 054**
	2015	61 995 478	165 383 576	**227 379 054**
Crédits de paiement	2019	97 206 797	265 285 961	**362 128 579**
	2018	89 674 675	263 395 690	**353 070 365**
	2017	80 513 246	165 008 804	**245 522 050**
	2016	66 377 128	145 102 763	**211 479 891**
	2015	61 995 478	173 957 584	**235 953 062**

En euros.
Sources : 2015 2016 et 2017 autorisations et crédits consommés (rapport annuel de performances/loi de règlement), 2018 et 2019 : Projet annuel de performances/ projet de loi de finance, 2019. Des ajustements importants interviennent chaque année en cours d'exercice, et sont retracés en loi de règlement, notamment des décrets de virement au titre des dotations consacrées aux capacités techniques interministérielles, au développement de produits de sécurité nationaux, en partenariat avec le ministère de la défense, d'études amont liées au développement de ces projets, ou en vue du financement du data center de Rosny-sous-Bois.

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

	PLF 2018		PLF 2019	
	AE	*CP*	*AE*	*CP*
SGDSN	***256 460 516***	***258 184 463***	***280 414 526***	***264 038 530***
Titre2	77 054 258	77 054 258	83 387 271	83 387 271
Hors titre 2	179 406 258	181 130 205	197 027 255	180 651 259
Fonds spéciaux	***67 381 927***	***67 381 927***	***67 190 341***	***67 190 341***
GIC	***28 166 931***	***28 168 931***	***30 887 891***	***30 899 708***
Titre2	12 559 129	12 559 129	13 819 526	13 819 526
Hors titre 2	15 607 802	15 607 802	17 068 365	17 080 182
Total action 2	**352 009 374**	**353 733 321**	**378 492 756**	**362 128 579**

Sources : PLF 2018 et 2019

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. Elle permet 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).**

Elle complète, enfin, l'information 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, elle permet d'appréhender la gestion des établissements publics, **l'IHEDN et l'INHESJ,** dont il assure une grande partie du financement par le versement d'une contribution pour charge de service public.

A l'inverse du GIC, service à compétence nationale[1], 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), soit plus de 40% des crédits de l'unité opérationnelle SGDSN (opérateurs compris) et relève du même statut juridique[2], ne constitue pour autant ni un BOP autonome, ni une unité opérationnelle. Vos rapporteurs regrettent une nouvelle fois que, dans le Projet annuel de performances annexé au projet de loi de finances, comme dans le Rapport annuel de performances annexé au projet de loi de règlement, les crédits et les effectifs de l'ANSSI ne soient pas présentés de façon apparente. L'agence devrait faire l'objet du même traitement que le GIC, et bénéficier d'une ligne dans la ventilation par destination et titre (p. 44) et dans la ventilation des emplois (p. 49) de la justification au premier euro. Même si l'on peut comprendre que la fongibilité des crédits et des plafonds d'emplois entre le SGDSN et l'ANSSI peut constituer un avantage en gestion, l'absence de ventilation au sein des crédits du SGDSN ne permet pas à première lecture une bonne appréciation par la représentation nationale des efforts consentis par le Gouvernement dans le domaine de la cyberdéfense et à la bonne information du public. Vos rapporteurs ne rencontrent pourtant aucun obstacle à obtenir ces informations du SGDSN.

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

[2] *Décret n° 2009-834 du 7 juillet 2009 modifié.*

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. Il 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, chef 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 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. **Depuis les attentats terroristes de 2015, le CDSN se réunit à un rythme soutenu. Du 1er novembre 2017 au 31 octobre 2018, il aura tenu 45 réunions.**

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 et 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. Il 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.

3. Pilotage des stratégies interministérielles

Le SGDSN est en charge de coordonner la réflexion interministérielle sur les **questions d'ordre stratégique**, telles que 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 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 a réalisé en 2017 et début 2018 un exercice inédit de rédaction d'une **revue stratégique de cyberdéfense.**

La revue stratégique de cyberdéfense

Entrepris par le SGDSN sur la base d'un mandat confié par le Premier ministre, la *Revue stratégique de cyberdéfense* a fait l'objet d'un examen en Conseil de défense et de sécurité nationale et d'une communication en Conseil des ministres le 8 février 2018.

Elle est l'aboutissement d'un important travail interministériel de réflexion et de consultation.

Organisée en trois parties, la *Revue stratégique de cyberdéfense* dresse un panorama de la cybermenace, formule des propositions d'amélioration de la cyberdéfense de la Nation et ouvre des perspectives visant à améliorer la cybersécurité de la société française.

1- La première partie de la *Revue* offre une analyse globale des dangers du monde cybernétique. Le paysage international apparait caractérisé par le développement de capacités offensives, notamment par un petit nombre de puissances bien identifiées, et par un cadre de régulation encore incomplet, dont les fondements théoriques doivent être confortés ; la France, à cet égard, a manifesté son rejet du « *hack back* » et s'est engagée en faveur de la responsabilisation des Etats dans la lutte contre les cyberattaques fomentées depuis leur territoire.

2- Mettant en avant l'Etat comme responsable de la cyberdéfense de la Nation, la deuxième partie s'attache à consolider le modèle français de cyberdéfense, fondé sur la séparation des fonctions offensives et défensives, ces dernières étant assurées, au premier chef, par l'ANSSI.

La *Revue* trace en outre le cadre doctrinal et d'organisation de la cyberdéfense française. Elle appelle à la mise en place de quatre chaines opérationnelles pour remplir ces missions : protection, action militaire, renseignement et investigation judiciaire.

3- La troisième partie met en avant le concept de souveraineté numérique, entendue comme le fait de conserver une capacité autonome d'appréciation, d'action et décision dans le domaine cybernétique, tout en protégeant d'autres composantes de la souveraineté nationale face aux nouvelles menaces engendrées par la numérisation. Cette souveraineté doit reposer sur la maitrise de certaines technologies telles que le chiffrement, et sur la consolidation d'une base industrielle nationale ou européenne.

http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

Il coordonnait les travaux du groupe interministériel sur la **dissémination des armements conventionnels.** Cette mission est désormais dévolue au comité de pilotage du programme européen[1] d'assistance à la mise en œuvre du Traité sur le commerce des armes, créé en 2017.

[1] *L'administration appuie Expertise France (EF), agence de mise en œuvre du programme européen, aux côtés du BAFA allemand, et a mis en place un comité qui détermine le contenu de l'assistance offerte par EF, oriente et organise la participation des différents experts français (des administrations et de la société civile) durant les trois années du programme. D'un montant de plus*

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**.** Il assure le secrétariat de diverses instances en charge de **coordonner les évaluations et les moyens de réduire les menaces chimique et biologique** 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 **le dispositif de protection du potentiel scientifique et technique de la nation (PPST)**. À ce titre, il reçoit les demandes de création et autorise la prise des arrêtés de création des zones à régime restrictif (*ZRR)*, par les ministères concernés. À ce jour, plus de 700 ZRR ont été créées générant plus de 24 000 demandes d'accès par an.

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*).

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]. Il participe, en outre, aux travaux internationaux sur les biens à double usage[2] et apporte

de 7 millions d'euros, ce programme permet de proposer une assistance sur mesure à une trentaine d'Etats afin de renforcer leurs capacités de contrôle des transferts d'armement (exportation, importation, transit, transbordement et courtage).

[1] *Loi n° 2011-702 du 22 juin 2011*

[2] *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.*

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

Activités de la CIEEMG

Sur la période d'août 2017 à août 2018, la CIEEMG s'est prononcée sur 6 326 dossiers correspondant à 5 062 dépôts de nouvelles « demandes de licence » et 1 264 demandes de « modification de licences » déjà accordées (soit 20% environ). Environ 92% des demandes ont fait l'objet d'un traitement en procédure « continue »[1] avec avis favorable. 58% des demandes de licence ou de modifications de licence ont été accordées avec des conditions particulières destinées à encadrer l'opération.

Elle s'est réunie en session plénière à onze reprises pour l'examen de 517 nouveaux dossiers, soit deux fois plus que sur la précédente période de douze mois, pour lesquels elle a prononcé 388 avis favorables et 117 avis défavorables[2].

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

1. La rénovation des plans de protection de la « famille pirate » dont le plan *Vigipirate* de lutte contre le terrorisme

Le plan *Vigipirate* du 1er décembre 2016[4] repose sur un système de niveaux[5] plus cohérent et mieux adapté à la menace, la mise en œuvre de nouvelles mesures renforçant l'action gouvernementale dans la lutte contre le terrorisme[6] et le développement d'une culture globale de la sécurité. Ce

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

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

[3] http://circulaire.legifrance.gouv.fr/pdf/2015/06/cir_39748.pdf

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

[5] *Il 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** » en cas de menace imminente ou suite à un attentat, limité à la durée d'activation de la cellule de crise, avec des mesures exceptionnelles de protection à leur plus haut niveau d'intensité.*

[6] *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, mais aussi, depuis 2018, la prise en compte de la loi sur la sécurité intérieure et la lutte contre le terrorisme avec la possibilité de mettre en*

dernier volet a donné lieu à un important travail de rédaction de guides et de fiches pratiques en 2018 et à de nombreuses actions de sensibilisation[1].

Depuis son entrée en vigueur, ce nouveau plan a démontré son adéquation avec les attentes des services de l'Etat, des collectivités territoriales, des opérateurs privés et publics. Au regard des menaces actuelles, il a permis la mise en œuvre de dispositions *ad hoc* de prévention et de réponses à une situation de crise de nature sécuritaire. Un exercice gouvernemental Vigipirate a été organisé en mai 2018.

Par ailleurs, après la validation des plans « *NRBC* » en décembre 2016, « *Piranet* » en cas d'atteinte majeure à la continuité des systèmes d'information liés aux activités vitales de la Nation, « *PirateMer* » de réaction à un acte de piraterie, de brigandage ou de terrorisme en mer et « *Piratair-Intrusair* » de réponse en cas d'acte illicite mettant en jeu la sûreté ou la souveraineté aérienne révisés en 2017, le SGDSN a finalisé le plan gouvernemental « *Pirate Mobilités Terrestres* » de réaction à un acte de terrorisme dans le domaine des transports terrestres. Celui-ci a fait l'objet d'un exercice gouvernemental en janvier 2018. Avec un périmètre élargi à tous les transports terrestres et à l'ensemble du territoire national, ce plan se substituera au plan « *Metropirate* » de 2008.

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

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 *CGI*, diffusé en février 2015 sous forme d'une instruction générale interministérielle, 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[2].**

---

place des périmètres de protection aux abords de certains lieux et d'événements, la fermeture administrative des lieux de culte ou encore l'extension des périmètres des contrôles administratifs, et la révision par ANSSI du domaine et des mesures cybernétiques.

[1] *Publication de guides de bonnes pratiques : http://www.sgdsn.gouv.fr/publications/ à destination des exploitants et des personnels de certains types d'établissements ou des organisateurs de grands évènements recevant du public, ainsi que les fiches pratiques annexées aux notes de posture, mise en place d'un dialogue national de sécurité. Il s'agit de cycles de rencontres visant à promouvoir les échanges entre les pouvoirs publics et les représentants de secteurs professionnels jugés sensibles (opérateurs des centres commerciaux en 2017, des festivals et des grands événements en 2018), en dehors des opérateurs d'importance vitale (OIV) pour lesquels un cadre d'échange existe déjà. La transmission de la note de posture est l'occasion de diffuser une vidéo de sensibilisation sur les réseaux sociaux.*

[2] *Fixées dans un cadre de juste suffisance et de complémentarité avec les autres acteurs de la gestion des crises (armées, collectivités territoriales et OIV), il comprend une partie générale et deux volets dédiés à la sécurité des systèmes d'information et à la réponse aux menaces NRBC.*

Sa déclinaison territoriale sous la forme d'un Contrat territorial de réponse aux risques et aux effets potentiels de menaces est en cours, sous le pilotage du ministère de l'intérieur. Une réunion interministérielle fin 2018 fera le point des actions et des engagements financiers réalisés par chaque ministère et de ceux projetés pour 2019.

A la suite de l'exercice gouvernemental « *Crue de Seine 2016* » et à la lumière du retour d'expérience relatif à l'épisode de crues traversé par l'Ile-de-France entre le 1er et le 7 juin 2016, le SGDSN a procédé à la révision du plan de continuité du travail gouvernemental en cas de crue majeure de la Seine à Paris. Ce plan a été validé en juillet 2017. Le dernier épisode de crue de janvier 2018 a permis de confirmer sa pertinence.

En outre, le SGDSN a piloté, en lien avec la direction générale de l'administration et de la fonction publique, une étude sur la mise en œuvre de conditions de travail exceptionnelles des agents des ministères en cas de crise majeure[1].

Enfin, le SGDSN a initié l'élaboration d'un plan d'action pour le renforcement de la logistique interministérielle de crise afin de coordonner les moyens des différents ministères face à des crises majeures de différentes natures susceptibles de survenir sur l'ensemble du territoire national[2].

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

Outre la création de guides et de fiches annexés aux notes de posture de protection du plan « *Vigipirate* », la révision des plans « *Crue de Seine* », « *Piratye-Mer* », « *Piranet* » *et* « *Piratair* », et la finalisation du plan « *Pirate Mobilités Terrestres* », le SGDSN a été mobilisé, en 2017 et 2018, autour de trois axes :

a) Les capacités liées à la protection du territoire national

Suite à un important travail interministériel, 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

---

[1] *Les principales recommandations portent sur l'harmonisation du cadre juridique du télétravail entre le secteur privé et la fonction publique, ainsi que sur l'adoption d'une disposition législative permettant le recours au télétravail en cas de circonstances exceptionnelles pour les agents de la fonction publique.*

[2] *A cet effet, le SGDSN met en place un groupe d'experts logisticiens afin d'étudier à froid les meilleures solutions susceptibles d'être mises en œuvre en cas de crise. En situation de crise, la cellule interministérielle de crise (CIC) pourra s'appuyer sur une cellule de coordination interministérielle logistique (CCIL), armée spécifiquement pour répondre à l'événement.*

du contrôle et de l'accompagnement des opérateurs, développement des patrouilles armées dans les transports. Pour optimiser la coordination et le pilotage politique des enjeux, les actions sont passées en revue par domaine, à l'occasion des réunions des commissions *ad hoc*[1] depuis 2018.

Les **transports terrestres** constituent une cible privilégiée des attaques terroristes à fort impact médiatique (Gares de Madrid en 2004, stations de métro et bus de Londres en 2005, aéroport de Bruxelles-National en 2016). Le SGDSN a réalisé le plan « *Pirate Mobilités Terrestres* » et a piloté, avec la SNCF, des travaux interministériels relatifs au traitement des colis abandonnés au sein de gares. Le protocole SNCF de traitement d'un objet abandonné a été validé en CISTTer. Cette commission a demandé la préparation des doctrines d'emploi et des modalités d'examen par l'Etat des performances des unités cynotechniques en vue de disposer d'une capacité cynotechnique privée encadrée à l'horizon de 2024. Le SGDSN participe aussi aux travaux interministériels consacrés à la vidéosurveillance « intelligente » *en particulier à travers les expérimentations conduites dans le cadre du projet de vidéoprotection ouverte intégrée (VOIE) soutenu par le comité de la filière industrielle de sécurité (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. Cela se traduit notamment par l'évaluation des vulnérabilités de ces espaces ouverts au public (aéroports de Strasbourg, Bordeaux et Orly en 2018, Lyon, Marseille, Lille, Montpellier et La Réunion en 2019), le déploiement d'équipes cynotechniques de détection d'explosifs et l'expérimentation de nouveaux matériels permettant la détection de menaces spécifiques telles que les armes longues. 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 dans le courant du premier semestre 2019 d'un système automatisé.

Enfin, le SGDSN pilote les travaux permettant de décliner les dispositions relatives à la loi n° 2016-1428 du 24 octobre 2016 relative au renforcement de la sécurité de l'usage des drones civils. Parallèlement, afin de lutter contre l'usage malveillant de ces appareils, il conduit les réflexions sur le cadre d'emploi des dispositifs de brouillage.

Dans le domaine de la **sûreté maritime et portuaire**, l'évaluation de la menace terroriste a été mise à jour en 2018. En complément des dispositions prises par les ministères impliqués, le SGDSN pilote, en liaison avec le secrétariat général de la mer (SGMer), les échanges avec les Etats côtiers de destination des navires à passagers sous pavillon français et plus particulièrement avec le Royaume-Uni. Conformément aux annonces du sommet de Sandhurst en janvier 2018, le SGDSN, avec les ministères concernés et les autorités britanniques, travaille à l'élaboration d'un accord intergouvernemental consacré à la sûreté maritime et portuaire en Manche et en mer du Nord. De la même façon, au second semestre 2018, le SGDSN va lancer des travaux afin de rechercher des accords de sûreté maritime avec la Tunisie et l'Algérie. Enfin, en juin 2018, le SGDSN a diffusé l'instruction interministérielle relative à l'organisation et à la coordination de la sûreté maritime et portuaire.

[1] *La commission interministérielle de la sûreté des transports terrestres (CISTTer), la commission interministérielle de la sûreté aérienne (CISA), et la commission interministérielle de sûreté maritime et portuaire (CISMaP),*

c) La consolidation des dispositifs interministériels de prévention et de protection

Le SGDSN finalise le renforcement de la politique de sécurité des activités d'importance vitale (SAIV) par la révision des directives nationales de sécurité (DNS). Ces travaux intègrent une approche « tous risques », incluant la planification de la continuité des activités face à un large éventail de risques et de menaces, et le renforcement de la sécurité des systèmes d'information, en étroite collaboration avec l'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* ». 40 sites[2] ont été identifiés comme pouvant être désignés PIV (points d'importance vitale) en plus des 60 existants. Les procédures de désignation sont en cours. Une offre spécifique de solutions de sécurité pourra être proposée aux exploitants de sites *Seveso*[3].

d) Le plan d'action contre le terrorisme

Le dispositif de prévention de la radicalisation et de lutte contre le terrorisme fait désormais l'objet d'approches distinctes et complémentaires grâce à la rédaction de deux plans thématiques : le plan national de prévention de la radicalisation (PNPR) et le plan d'action contre le terrorisme (PACT).

Le SGDSN, en liaison étroite avec la coordination nationale du renseignement et de la lutte contre le terrorisme, a assuré la coordination des travaux interministériels qui ont abouti en juillet dernier à la rédaction du PACT qui constitue la feuille de route des pouvoirs publics dans la lutte contre le terrorisme pour les deux années à venir.

Ce plan identifie 32 actions publiques et 8 non publiques, à mener dans cinq domaines prioritaires : connaître (mieux identifier et comprendre la menace terroriste et ses évolutions) ; entraver (prévenir et empêcher les passages à l'acte) ; protéger (adapter les dispositifs de protection des personnes et des biens) ; réprimer (optimiser les politiques de répression et le traitement judiciaire) ; l'Europe qui protège (accroître les synergies entre les États membres et promouvoir les initiatives au sein de l'Union). Le SGDSN suivra sa mise en œuvre et pilote directement six actions du PACT.

[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 ».*

[3] *Une première expression du besoin du CoFIS portait sur la détection d'armes et d'explosifs à l'entrée de l'installation, la détection, la localisation et le suivi d'intrus. Sur la base de cette expression de besoin, une méthodologie d'analyse du besoin capacitaire a été proposée et est en cours d'expérimentation. Un premier catalogue d'une trentaine de solutions existantes a été proposé par le conseil des industries de la confiance et de la sécurité (CICS) à l'union des industries chimiques (UIC) et à l'union française des industries pétrolières (UFIP). Un projet porté par des PME sur le suivi et la traçabilité des intervenants sur un site sensible type Seveso est actuellement financé dans le cadre de l'appel à projets sécurité du deuxième programme d'investissements d'avenir (PIA2).*

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. Une importante concertation interministérielle est menée, sous le pilotage du SGDSN, pour actualiser les dispositions réglementaires du code de la défense, du code de procédure pénale et du code des postes et des communications électroniques.

Une finalisation des travaux rédactionnels est envisagée d'ici la fin de l'année 2018. L'objectif est de rénover la protection du secret autour de trois priorités : ajuster les niveaux de classification en passant de trois à deux niveaux ; améliorer la prise en compte de l'information classifiée dématérialisée et renforcer la protection des systèmes d'information classifiés ; procéder à des ajustements techniques et juridiques.

La préservation du secret repose sur l'action d'un réseau de 4 000 officiers de sécurité et sur la responsabilité des 400 000 personnes habilitées en France. V**otre 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.

La formation à la protection du secret de la défense nationale

Au sein de chaque organisme détenant des informations et supports classifiés, **l'officier de sécurité et, le cas échéant, l'officier de sécurité des systèmes d'information, sont chargés**, d'une part, **de former le personnel habilité** aux règles de la protection du secret et, d'autre part, **de le sensibiliser aux menaces** d'investigation ou d'approches par des individus ou des organisations étrangères et aux risques spécifiques encourus hors du territoire national.

Ces officiers de sécurité bénéficient d'une formation adaptée. L'Institut national des hautes études de la sécurité et de la justice (INHESJ) a mis en place, en partenariat avec le SGDSN, une formation interministérielle. Les trois premières sessions se sont déroulées en 2018, au profit d'une centaine d'officiers de sécurité des secteurs public comme privé.

Parallèlement, le SGDSN participe régulièrement aux séminaires internes des ministères comme aux sessions des instituts de formation, apportant l'éclairage spécifique sur les enjeux de protection du secret de la défense nationale. D'autres actions destinées à améliorer le dispositif global de formation ont également été menées, tel que la mise en ligne sur son site internet d'un test de connaissance dédié à la protection du secret ou la conception d'une plaquette de sensibilisation. Ces outils, en accès libre, contribuent à développer une culture de sécurité.

Au-delà de ces formations en continu, l'intégration des enjeux de la protection du secret de la défense nationale au sein des formations initiales est un effort en cours. A ce stade, le SGDSN intervient essentiellement dans le cadre de la formation dispensée par l'ENA aux élèves reçus au concours d'entrée.

Vos rapporteurs saluent cet effort. Ils insistent également pour 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 au-delà de la seule ENA.

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

Le secteur français des industries de sécurité représente un chiffre d'affaires de 30 milliards d'euros (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[2].

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

Pour mettre en œuvre la politique du Gouvernement en matière de sécurité des systèmes d'information[3], le SGDSN dispose de l'ANSSI[4]. Ce positionnement de l'Agence 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 et de rendre plus complexe l'analyse des emplois et crédits dans le programme annuel de performance (voir supra p.8).

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.

La *Revue stratégique de cyberdéfense*[5] trace le cadre doctrinal et d'organisation et s'attache à consolider le modèle français, fondé sur la séparation des fonctions offensives et défensives, ces dernières assurées, au premier chef, par l'ANSSI. Le dispositif législatif de la LPM 2019-2025 a

---

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

[2] *Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 17 et suiv.* http://www.senat.fr/rap/a17-110-9/a17-110-96.html#toc105 *et* https://www.gouvernement.fr/le-cofis-au-travail-3224

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

[4] *Service à compétence nationale (décret n° 2009-834 du 7 juillet 2009 modifié).*

[5] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

élargi ses missions. Le rapport d'activité 2017 de l'ANSSI donne une vision détaillée des missions actuelles et à court terme[1].

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

Les attaquants informatiques poursuivent quatre types d'objectifs non exclusifs entre eux : l'espionnage, les trafics illicites, la déstabilisation et le sabotage[2]. Dans son rapport d'activité, l'ANSSI constate que « *l'année 2017 aura été marquée par de nombreuses attaques cybernétiques, inédites par leur ampleur, leur mode de diffusion et leur caractère désormais non-discriminant* ».

Le rapport met en exergue :

• la publication d'outils d'attaques sophistiqués qui facilite leur duplication à l'infini et leur diffusion rapide, venant ainsi grossir les arsenaux des groupes malveillants et rendre .plus difficile voire impossible l'identification de l'origine des attaques ;

• une recrudescence d'attaques aux effets destructeurs réalisées à des fins lucratives ou de sabotage. Parmi elles, l'agence observe depuis 2014 une hausse constante des attaques par rançongiciel, de virulence variable ;

• l'espionnage par compromission d'éditeurs ou de prestataires informatiques afin d'obtenir à l'insu de la cible un avantage stratégique par le recours à des outils et modes opératoires adaptés au niveau de sécurité du système d'information ciblé. En 2017, ces opérations se sont particulièrement illustrées par leur caractère indirect avec des attaques visant notamment la chaîne d'approvisionnement de l'entreprise ciblée.

Outre la persistance de ces menaces, l'ANSSI a relevé en 2018 :

• de nombreuses vulnérabilités critiques affectant des composants et des équipements informatiques grand public pouvant affecter un nombre très important de systèmes d'information ;

• des cas de ciblage aux fins de déstabilisation, des grands événements internationaux en raison de leur forte médiatisation, ainsi que des actions de déstabilisation à grande échelle, qui peuvent s'appuyer sur la compromission de systèmes d'information, afin de recueillir et divulguer massivement des données sensibles, notamment dans le cadre d'élections ;

• des attaques sont menées afin d'utiliser, à l'insu de leurs propriétaires, la puissance de calcul d'équipements compromis pour « miner » des cryptomonnaies.

Le rapport Symantec[3] confirme l'analyse de l'ANSSI, donne des statistiques précises sur les cyberattaques et classe la **France désormais au 9ème rang mondial (et au 4ème rang) européen des pays où la cybercriminalité est la plus active.**

---

[1] https://www.ssi.gouv.fr/uploads/2018/04/rapport_annuel_2017_anssi.pdf

[2] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf *p.11 à 26*

[3] Symantec *Internet Security Threat Report (ISTR)* https://www.symantec.com/fr/fr/security-center/threat-report

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.

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.

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 est poursuivie par les recommandations des revues stratégiques de la défense d'octobre 2017[2] et de cyberdéfense de février 2018[3] et les dispositions incluses dans la LPM 2019-2025.

C. LE RENFORCEMENT DU CHAMP DES COMPÉTENCES DE L'ANSSI

L'ANSSI est l'autorité nationale en matière de sécurité et de défense des systèmes d'information. Dès sa création en 2009, les missions de préparer la France à des attaques informatiques majeures[4] et de se doter d'une capacité de détection d'attaques informatiques lui ont été confiées.

Depuis 2014, des missions en matière de protection des systèmes d'information des opérateurs d'importance vitale (OIV) ont été attribuées à l'ANSSI. Ce champ de compétences a été étendu au cours de l'année 2018 par les conclusions de la *Revue stratégique de cyberdéfense (RCS)*[5] ainsi que par les dispositions de la LPM 2019-2025 et les dispositions issues de la transposition de la directive *NIS*.

La *RCS* émet de nombreuses recommandations qui s'inscrivent majoritairement dans la continuité des travaux stratégiques nationaux précédents – et notamment de la stratégie nationale pour la sécurité du numérique de 2015[6].

Leur mise en œuvre est pilotée par le SGDSN[7]. Du point de vue de l'ANSSI, certains des chantiers dont elle assure le pilotage ou le co-pilotage,

---

[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] *http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf*

[4] *Comparables à celle subies par l'Estonie en 2007*

[5] *Voir encadré supra p.10.*

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

[7] *À ce titre, une première réunion tenue en mars 2018, sous la présidence du SGDSN et en présence du cabinet du Premier ministre a abouti à l'élaboration d'un tableau de suivi de plus de 80 recommandations. Une deuxième réunion le 24 mai a préparé la première réunion du comité de*

ou dans lesquels elle est significativement impliquée, sont particulièrement structurants. On compte désormais parmi ses missions de l'ANSSI :

- le déploiement de **moyens de prévention, de veille, de réaction et de détection** des attaques informatiques, la gestion des crises et l'assistance aux administrations ou OIV victimes d'attaques informatiques. A cet effet, l'agence est amenée à conduire des activités opérationnelles permanentes. La LPM 2019-2025 lui a confié de nouvelles prérogatives en matière de détection des attaques informatiques[1] ;
- la **contribution au dispositif permanent de suivi de la menace et de gestion interministérielle des incidents de sécurité informatique**. Les réflexions menées dans le cadre de la rédaction de la *RCS* ont conduit à la mise en place d'un centre de coordination des crises cyber (C4)[2] ;
- **l'accompagnement et le soutien technique** aux services de l'Etat et aux OIV. L'ANSSI assure ainsi un rôle de vivier d'expertise de haut niveau. La *RCS* prévoit notamment que l'ANSSI puisse donner son avis sur les projets informatiques les plus importants et les plus sensibles de l'Etat ;
- **l'élaboration et la mise à jour de la réglementation** relative à la sécurité numérique, notamment en ce qui concerne les OIV et les opérateurs essentiels au fonctionnement de l'économie et de la société[3] ;
- le maintien à l'état de l'art des **expertises scientifiques et techniques** nécessaires dans tous les domaines liés au numérique, en lien avec les acteurs publics et privés de l'écosystème. A ce titre, l'ANSSI conduit des activités de recherche scientifique et technique ;
- **la représentation de la France**, en lien avec les ministères compétents, dans les organisations internationales, le suivi des négociations internationales sur les questions susceptibles d'avoir un impact en matière de sécurité numérique, et l'établissement de partenariats, notamment opérationnels, avec d'autres pays ;
- la conception et le maintien en condition opérationnelle et de sécurité des **systèmes d'information gouvernementaux classifiés de défense interministériels**.

---

pilotage de la cyberdéfense (« COPIL cyber »), tenue fin juin, sous la présidence du cabinet du Premier ministre et a dressé un premier état de l'avancement des actions les plus significatives.

[1] *Rapport n° 476 (2017-2018) de M. Christian Cambon, sur le projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense fait au nom de la commission des affaires étrangères, de la défense et des forces armées, page 156 et suivantes* http://www.senat.fr/rap/l17-476/l17-47622.html#toc134.

[2] *Lancé en avril 2018, le C4 est un mécanisme interministériel permanent d'analyse de la menace, de préparation et de coordination, qui regroupe l'ensemble des acteurs concernés au-delà de la seule sphère technique, afin d'assurer l'échange des informations et analyses relatives aux attaques informatiques et de faciliter la préparation des options de réponse de l'Etat, tant sur les aspects techniques que diplomatiques ou judiciaires.*

[3] *L'extension du périmètre d'intervention de l'ANSSI pour la détection des cyberattaques aux opérateurs de service essentiels est la conséquence d'un amendement de la commission des affaires étrangères, de la défense et des forces armées du Sénat. Rapport n° 476 (2017-2018), page 173 et suivantes* http://www.senat.fr/rap/l17-476/l17-47622.html#toc134.

D. UNE CAPACITÉ D'EXPERTISE DE TRÈS HAUT NIVEAU

L'ANSSI constitue un vivier d'expertise au profit des services de l'Etat et apporte son soutien à de nombreux projets informatiques sensibles. Elle conduit dans sept laboratoires thématiques intégrés à la sous-direction *Expertise*[1], des activités de recherche scientifique et technique afin d'assurer le maintien à niveau des expertises nécessaires à tous les domaines liés au numérique, en lien avec les acteurs publics et privés de l'écosystème.

E. 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.

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 d'information de l'État* » (PSSIE)[2] **et des règles de protection**[3]. 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.

---

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

[2] *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.*

[3] *n° 5725/SG du 17 juillet 2014.*

Dans leur avis sur les PLF 2017[1] et 2018[2], vos rapporteurs s'inquiétaient de la lenteur de ce processus. Les résultats ne se sont guère améliorés. Le niveau effectif de conformité, qui fait l'objet d'un indicateur[3] sous l'objectif 6 du programme 129 « *améliorer la sécurité et la performance des systèmes d'information de l'Etat* », tarde toujours à atteindre des niveaux en adéquation avec les enjeux. « *Les constats d'audits menés en 2017 confirment que si certains ministères se sont appropriés la sécurité du numérique et ont adopté une posture adaptée aux multiples enjeux, la réalité des transformations numériques engagées et l'historique des systèmes d'information font que le niveau de maturité n'est pas souvent aussi élevé que celui estimé. Ce constat est d'autant plus flagrant pour les ministères disposant de moyens humains et financiers plus faibles* »[4].

Si l'on constate une meilleure prise en compte des enjeux par les autorités, celle-ci reste insuffisante. Cette situation consternante et alarmante a été confirmée par la *RCS*[5].

La sécurisation des systèmes d'information de l'État

Diagnostics et recommandations

Le niveau de sécurité réel des systèmes d'information de l'État demeure inégal et souvent trop faible, ce qui les expose à des attaques informatiques, y compris non ciblées menés par des attaquants aux compétences techniques limitées. Plusieurs axes d'amélioration peuvent cependant contribuer à pallier ces faiblesses.

Perfectionner la gouvernance de la cybersécurité

La visibilité de l'ANSSI et son pouvoir de contrôle des initiatives numériques ne suffisent pas pour lui permettre de veiller à la bonne prise en compte de la sécurité. Son expertise est souvent sollicitée à des phases trop avancées des projets informatiques ministériels ce qui génère d'importants surcoûts et rend difficile l'atteinte *in fine* du niveau de sécurité adaptés aux risques (...).

À ce jour, en application de l'article 3 du décret n° 2014-879 du 1er août 2014, l'ANSSI formule un avis relatif à la prise en compte de la sécurité informatique pour les grands projets de l'Etat (> 9M€)[6]. Afin d'étendre ce périmètre à l'ensemble des projets sensibles pour l'Etat, l'ANSSI (...) contribue à la création des directions du numérique (DINUM/DNUM), qui seront des partenaires privilégiés sur ce sujet.

Au sein des ministères, la gouvernance de la sécurité des systèmes d'information doit être renforcée. Les DSI ministérielles sont insuffisamment formées et peu responsabilisées dans ce domaine. Leurs processus de travail prévoient rarement un volet relatif à la sécurité des systèmes d'information et le risque cyber est souvent mal pris en compte (...). La revue recommande une responsabilisation des DSI ministériels (…) et le renforcement de leur formation.

---

[1] *Sénat n° 142 Tome IX (2016-2017) par MM., Bockel et Masseret, p. 37 et suiv.*

[2] *Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 24 et suiv.* http://www.senat.fr/rap/a17-110-9/a17-110-96.html#toc105

[3] *Indicateur 6-1 « Niveau de sécurité des systèmes d'information de l'Etat »*

[4] *Programme annuel de performance n°129 page 28 :* https://www.performance-publique.budget.gouv.fr/sites/performance_publique/files/farandole/ressources/2019/pap/pdf/PAP2019_BG_Direction_action_du_Gouvernement.pdf

[5] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf *page 56 et suiv.*

[6] *S'agissant des projets de nature opérationnelle du ministère des Armées, il revient au COMCYBER d'être saisi pour avis et de solliciter l'ANSSI en tant que de besoin.*

(..) Le dialogue entre les directions métier et les DSI ministérielles est perfectible. La responsabilité de la sécurité du socle informatique commun à l'ensemble d'un ministère (…) relève de la DSI du ministère, il appartient en revanche aux directions métier elles-mêmes de fixer les besoins de sécurité des outils et applications numériques développés au profit de leur métier, parfois sans une implication significative de la DSI. (…) La responsabilisation des directeurs d'administration quant à la sécurité des systèmes d'information métier apparait indispensable (…).

Un groupe de travail interministériel a été lancé le 6 septembre 2018. Ces travaux visent à augmenter le niveau de confiance dans les systèmes d'information de l'Etat : en aboutissant à une véritable culture de gestion des risques ; en clarifiant l'organisation et les responsabilités dans le domaine de la sécurité du numérique ; et en plaçant le numérique au cœur des réflexions des acteurs métier. Le rapport final sera livré à la fin de l'année 2018.

Optimiser l'utilisation du RIE à des fins de cyberdéfense

Renforcer la sécurité du système d'information de l'État est une des missions du Réseau interministériel de l'Etat (RIE). Il s'appuie sur une plateforme unifiée d'accès à Internet qui offre des services de sécurité centralisés. Elle est insuffisamment utilisée par certains ministères (…) ce qui réduit les capacités de cyberdéfense de l'Etat. Son utilisation généralisée permettrait à l'ANSSI de renforcer significativement son service de détection des attaques informatiques.

Le service à compétence nationale chargé de gérer ce réseau ne disposant pas des ressources et compétences nécessaires pour assurer la collecte et l'exploitation des métadonnées issue du RIE à des fins de cybersécurité, la Revue propose de « *confier à l'ANSSI la détection des attaques sur ce réseau* », (…).

L'ANSSI et la DINSIC ont élaboré une feuille de route portant sur la sécurité et les services de sécurité du RIE. Les actions initiées avant la rédaction de cette feuille de route et les travaux sur la supervision du RIE avancent suivant le calendrier prévu. En revanche, du fait des évolutions régulières des priorités et du manque de moyens du RIE, aucune autre action n'a été initiée et les priorités de la feuille de route doivent être renégociées.

Renforcer la supervision de la cybersécurité des services de l'État

L'ANSSI opère un service interministériel de supervision de la sécurité, qui s'appuie notamment sur des sondes de détection d'attaques informatiques positionnées sur les réseaux des ministères et sur le RIE. Le modèle actuel se heurte néanmoins à plusieurs limites : (…) plusieurs administrations ne font toujours pas l'objet d'une supervision de sécurité, ce qui limite de fait la capacité nationale de détection des attaques (…). En outre, ce dispositif n'est pas applicable aux services étatiques hébergés par des prestataires externes, (…) ; la tendance à l'externalisation des applications métier est donc susceptible, à droit constant, de remettre en question la capacité de détection des attaques informatiques.

La revue recommande d'imposer la couverture complète des services informatiques utilisées par l'État par un dispositif de supervision de sécurité, y compris dans les cas où ces services sont externalisés.

A l'heure actuelle, le taux de couverture des services informatiques utilisés par l'Etat – hors services externalisés – par un dispositif de supervision de la sécurité de l'ANSSI est estimé à 80%. Pour les ministères disposant de réseaux non supervisés, l'ANSSI va initier un dialogue avec plusieurs ministères (...).

Adapter la politique d'achat de l'État aux enjeux de sécurité informatique

Le recours à des produits et à des services de cybersécurité labellisés par l'ANSSI constitue un levier important pour assurer la sécurité des réseaux de l'État.

Cependant sa mise en œuvre se heurte à plusieurs obstacles, dont l'incompatibilité des cadres d'achat ministériels et interministériels avec l'acquisition de telles solutions et l'insuffisance des budgets ministériels dans de domaine[1], (…). Au-delà, les démarches générales d'achats de solutions informatiques par l'Etat devraient faire l'objet d'une attention particulière de sécurité afin de garantir a minima le respect des bonnes pratiques élémentaires pour tout nouvel outil numérique acquis. La revue recommande d'élaborer des clauses contractuelles types et d'inciter fortement les ministères à inclure ces clauses dans leurs marchés publics comportant un volet numérique.

Un groupe de travail a été lancé entre la DAE[2] et l'ANSSI et un plan d'action a été établi. Les premières conclusions sont attendues pour fin 2018.

Ce constat a pu être partagé dans le cadre des travaux interministériels du projet « *Action publique 2022* ». Plusieurs chantiers ont été lancés afin de renforcer le niveau de sécurité des systèmes d'information de l'État (voir les passages en gras dans l'encadré ci-dessus).

Vos rapporteurs se réjouissent de cette prise de conscience, mais ils estiment que sans portage politique majeur permanent, sans moyens financiers significatifs et sans outils réglementaires coercitifs, il sera difficile de lutter contre une logique qui valorise la multiplication de systèmes d'information et des applications numériques permettant d'abaisser des coûts de fonctionnement ou de personnels. Ils souhaitent que l'Etat fixe aux ministères la réalisation d'un ratio obligatoire d'investissement dans la cybersécurité et qu'en cas de non-respect de ce ratio, les crédits de développement informatique du ministère soient réduits de façon drastique ; qu'une formation solide évaluée par l'ANSSI soit imposée pour tout recrutement des nouveaux DSI ministériels et imposée aux directeurs « métiers »pilotant la mise en œuvre de projets numériques ; et que des objectifs en matière de sécurité informatique définis par l'ANSSI soient explicitement imposés dans leurs lettres de mission et pris en compte dans leur évaluation.

La *RCS* a affirmé une nouvelle ambition pour la France en matière de défense et de sécurité de ses systèmes numériques, avec des effets directs sur l'activité de l'ANSSI. Ces travaux supplémentaires ont été intégrés dans la progression globale des moyens pour l'année 2019.

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 :

---

[1] *L'inscription de certaines solutions labellisées par l'ANSSI dans les cadres a fortement facilité leur mise en œuvre comme l'acquisition par l'ANSSI en 2015 d'une licence globale libératoire pour les logiciels labellisés de la société* Prim'X *qui a permis* le *déploiement de 600 000 logiciels de chiffrement robuste au sein de l'administration.*

[2] *La direction des achats de l'Etat (DAE), direction d'administration centrale du ministère de l'action et des comptes publics, définit la politique des achats de l'Etat, sous l'autorité du Premier ministre. Elle s'assure également de sa mise en œuvre, après concertation avec les ministères.*

- 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).

Au-delà des programmes majeurs engagés, le SGDSN a poursuivi le financement d'un *data center en partenariat avec le ministère de l'intérieur*[1]. Le site sera pleinement opérationnel à partir de janvier 2019[2]. Le coût global des travaux dans le cadre du marché s'élève à 29,41 M€ dont 22,13 M€ pour le SGDSN, ce qui correspond à 75% des travaux communs auxquels s'ajoutent certains travaux spécifiques. Des coûts complémentaires de câblage et de sécurité s'élèvent à 3,44 M€.

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 OIV. 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. Il est chargé de la supervision des sondes déployées par l'ANSSI sur les réseaux étatiques d'intérêt pour la Nation. Ces dispositifs sont notamment positionnés sur le réseau interministériel de l'Etat (RIE). Enfin, il réalise plusieurs dizaines de prestations d'audit au profit de l'administration ainsi que des OIV privés[3].

Ce service de supervision a permis à l'ANSSI de détecter et de comprendre des attaques informatiques sophistiquées ciblant l'État. Le système actuel se heurte néanmoins à plusieurs limites :

- les dispositifs de détection sont principalement installés en périphérie des systèmes d'information des ministères. Ce positionnement restreint l'analyse aux échanges qui ont lieu entre les réseaux des bénéficiaires du service de supervision et le réseau Internet ; il ne permet généralement pas de détecter les activités malveillantes qui se déroulent au sein même des réseaux de l'Etat ;

---

[1] *Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 26 et suiv.* http://www.senat.fr/rap/a17-110-9/a17-110-96.html

[2] *Après 30 mois de travaux, la réception de l'infrastructure a eu lieu le 31 juillet 2018 et la mise en service est programmée pour la fin de l'année 2018, après des travaux complémentaires d'installation du matériel informatique.*

[3] *L'ANSSI a réalisé en 2017, 63 audits auprès des ministères et des OIV : 65% d'audits à la demande (60% en 2016), le reste à l'occasion d'opérations, dans le cadre d'inspections ministérielles ou à l'occasion de missions de contrôle. Sur l'année, les prestations d'audit ont bénéficié en premier lieu aux institutions, ministères et autorités indépendantes (58% de l'ensemble des audits) ; les OIV représentent près de la moitié des activités d'audit de l'agence.*

- les déploiements des dispositifs sont limités aux entités étatiques qui en ont fait la demande et sont effectués selon les modalités fixées par celles-ci, ce qui ne permet pas toujours à l'ANSSI d'installer des dispositifs de détection d'attaque dans des conditions adaptées à la menace ;
- en phase d'exploitation, les ministères ne disposent que de ressources limitées pour répondre aux sollicitations de l'ANSSI, ce qui ne permet pas d'assurer un service de détection optimal.

Parallèlement, l'article 34 de la LPM 2019-2025 a introduit deux mesures concourant à l'amélioration de la capacité nationale de détection. :

- permettre aux opérateurs de communications électroniques de mettre en œuvre des dispositifs de détection des attaques informatiques affectant les systèmes d'information de leurs abonnés sur lesquels l'ANSSI pourra s'appuyer[1].
- donner à l'ANSSI la capacité de déployer ses propres dispositifs de supervision de la sécurité chez les opérateurs et les hébergeurs[2] afin d'être en mesure d'acquérir la connaissance nécessaire à l'anticipation des nouvelles menaces et à la compréhension des modes opératoires d'attaques, pour, *in fine*, mieux les contrer. L'Autorité de régulation des communications électroniques et des postes (ARCEP) est désignée comme autorité de contrôle de la mise en œuvre de ces dispositions.
- Sur le plan financier, les dispositifs de détection déployés par les opérateurs de communications électroniques demeurent à leur charge. L'exploitation des marqueurs techniques fournis par l'ANSSI fera l'objet d'une juste rémunération, dont le niveau sera fixé par arrêté. Le déploiement de dispositifs par l'ANSSI sur les réseaux des opérateurs et des hébergeurs en fera également l'objet. **Le coût pour l'Etat sur 2019 restera marginal, car le déploiement de ces dispositifs sera très progressif et les dépenses générées chez les opérateurs resteront très faibles (électricité consommée et espace occupé).**

F. L'ÉLARGISSEMENT DU PÉRIMÈTRE D'ACTION

La LPM 2014-19 et la stratégie numérique de 2015 ont fixé des orientations et priorités en matière de protection des systèmes d'information des OIV et d'assistance aux victimes des actes de cyber malveillance. L'ANSSI les accompagne dans la sécurisation de leurs systèmes d'information critiques qui passe, entre autres, par l'application de règles de sécurité qu'elle définit avec les opérateurs, ainsi que par l'installation d'un dispositif de détection d'incidents et d'attaques.

---

[1] *L'ANSSI peut transmettre à ces opérateurs des marqueurs techniques, qu'ils exploitent au sein de ces dispositifs de détection. Ils alertent l'ANSSI lorsque des incidents de sécurité sont détectés et, à sa demande, lui communiquent des données techniques permettant de comprendre les modes opératoires des attaquants et d'identifier les victimes. A la demande de l'ANSSI, ils informent leurs abonnés de la vulnérabilité ou de l'atteinte de leurs systèmes d'information.*

[2] *Sur un périmètre et pour une durée limités lorsque la sécurité des systèmes d'information des opérateurs d'importance vitale, des opérateurs de services essentiels ou des autorités publiques est menacée.*

La directive européenne relative à la sécurité des systèmes d'information, dite NIS, transposée par une loi du 26 février 2018[1], conforte ces orientations. La mise en place de la notion d'opérateurs de services essentiels (OSE) permettra d'englober des entités au-delà des actuels OIV.

1. Une assistance aux OIV soutenue par un dispositif réglementaire

L'article 22 de la LPM 2014-2019 a défini un cadre réglementaire imposant un renforcement de la sécurité des systèmes d'information des OIV. Il en existe aujourd'hui plus de 200, répartis en 12 secteurs d'activités. Sa mise en œuvre s'est poursuivie depuis 2014, et l'ANSSI a publié en 2017 les derniers arrêtés sectoriels. En 2017, pas moins de 1 000 systèmes d'information d'importance vitale ont été déclarés à l'ANSSI.

Elle 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)[2].

Cet élargissement conduira à renforcer les structures de coordination, de conseil mais également de contrôle et d'assistance opérationnelle[3]. **L'ANSSI se positionne 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 OIV 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 de création d'un objectif du PAP et d'un indicateur permettant de mesurer de façon synthétique les progrès réalisés en fonction de cibles à atteindre, et que soit publié un tableau de bord annuel synthétique sur les infractions constatées et les mesures de remédiation réalisées.**

2. La transposition de la directive NIS

L'enjeu de la directive adoptée, le 6 juillet 2016, est d'assurer un niveau élevé et commun de sécurité dans l'UE[4]. Depuis l'adoption de la loi

---

[1] *Loi n°2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité*

[2] *Le décret n° 2015-350 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale en précise les conditions de délivrance.*

[3] *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.*

[4] *Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 33 et suiv.* http://www.senat.fr/rap/a17-110-9/a17-110-96.html

n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité, et notamment de ses articles 5 à 9, les opérateurs, publics ou privés, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux et systèmes d'information nécessaires à la fourniture desdits services (OSE), désignés par le Premier ministre sont soumis à des règles de sécurité élaborée par l'ANSSI.

Ces règles ont pour objet de garantir un niveau de sécurité adapté au risque existant, de prévenir les incidents qui compromettent la sécurité des réseaux et systèmes d'information utilisés pour la fourniture des services essentiels. Les OSE, dont le nombre est estimé à quelques centaines, sont tenus à effectuer auprès de l'ANSSI la déclaration des incidents affectant leurs réseaux et systèmes d'information[1] et ils peuvent être soumis à des contrôles du respect de ces obligations[2]. Ces règles sont voisines de celles imposées aux OIV visés par les articles L. 1332-1 et L. 1332-2 du code de la défense.

Sur proposition de votre Commission, le périmètre des conditions permettant à l'ANSSI de détecter ou de caractériser une cyberattaque à travers le système de détection sur les réseaux des opérateurs de communication électronique et les serveurs des fournisseurs d'accès à des services de communications électroniques, a été étendu dans la LPM 2019-2025 aux menaces susceptibles de porter atteinte à la sécurité des systèmes d'information des OSE. Ces opérateurs bénéficieront du dispositif de détection sans que cela représente pour eux une charge supplémentaire.

Est introduit également un volet destiné à renforcer la cybersécurité des fournisseurs de services numériques qui seront tenus d'assurer la sécurité de leurs services et de notifier leurs incidents à l'ANSSI.

En conséquence, la loi a accru fortement le nombre d'acteurs régulés et susceptibles d'être assistés prioritairement en cas d'attaque. **Un renforcement des effectifs de l'ANSSI sera nécessaire pour se saisir des nouvelles prérogatives : traitement des signalements d'incidents en provenance des OSE, accompagnement de ces opérateurs, *etc*.**

3. 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

[1] *Nécessaires à la fourniture de services essentiels, lorsqu'ils ont ou sont susceptibles d'avoir un impact significatif sur la continuité de ces services, sous peine de sanctions pénales*

[2] *Et, en cas de manquement, l'ANSSI peut mettre en demeure les dirigeants de l'opérateur concerné de se conformer aux obligations qui incombent à l'opérateur*

commercialisation et la détention d'équipements susceptibles de porter atteinte à la confidentialité des communications électroniques[1].

4. 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. L'ANSSI est également partie prenante dans la planification et le jeu des exercices « Defnet », organisés sous la responsabilité du ministère des armées[2].

5. 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.

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 référencés susceptibles de les accompagner dans le traitement des incidents de sécurité informatique[3], copilotée par le ministère de l'intérieur.

En une année de fonctionnement, la plateforme a déjà enregistré les déclarations de 25 000 victimes dont 85% de particuliers, 12% d'entreprises et 3% de collectivités et a référencé quelque 1 600 prestataires. Avec cette masse critique, la plateforme propose à chaque appel à l'aide une moyenne de 28 prestataires de proximité. Ceux-ci ont rédigé 276 rapports d'intervention.

---

[1] *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.*

[2] *La série des exercices DEFNET constitue l'entraînement majeur de la chaîne militaire de cyberdéfense du ministère des armées qui l'organise pour son compte propre. L'ANSSI a été observateur lors de l'édition 2018 de l'exercice et prévoit une participation plus marquée en 2019, dans le cadre du partenariat en matière de défense des systèmes d'information entre l'ANSSI et le commandement de la cyberdéfense (COMCYBER) du ministère des armées.*

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

L'autre mission de Cybermalveillance.gouv.fr est la sensibilisation des particuliers et des professionnels à la cybersécurité et la diffusion de bonnes pratiques pour se protéger. Le premier volet de son kit de sensibilisation a été téléchargé 17 000 fois. Une nouvelle version proposera un suivi plus complet de la relation entre la victime et le prestataire jusqu'à l'évaluation de ce dernier.

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

Lancée en mai 2017, **le MOOC SecNum*academie*** a pour objectif de permettre aux étudiants, salariés, dirigeants d'entreprise ou particuliers d'être initiés à la cybersécurité ou d'approfondir leurs connaissances afin de pouvoir agir efficacement sur la sécurité de leurs systèmes d'information. Gratuit et accessible à tous, il donne accès à un large contenu pédagogique proposé et conçu par les experts de l'ANSSI. Fin 2017, la plateforme comptait près de 50 000 inscrits. La formation est sanctionnée par une attestation de réussite obtenue par la validation progressive des crédits attribués.

Pilotée par l'ANSSI[2], **la certification SecNum*edu*** apporte aux étudiants et employeurs la garantie que la formation répond à une charte et des critères définis par l'ANSSI en collaboration avec les acteurs et professionnels du domaine. Elle vise à apporter de la lisibilité à l'offre de formation et aux métiers du secteur et à leur offrir davantage de visibilité. Plus de 40 établissements de formation initiale et continue ont reçu ce certificat.

L'ANSSI propose également une **labellisation des formations d'enseignement supérieur mettant en œuvre les principes de sa démarche pédagogique en matière de sécurité du numérique.** En juin 2017, Cyber*Edu* a lancé son processus de labellisation. À ce jour, 7 formations ont reçu le label[3].

Elle met enfin 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, les chambres consulaires et des entreprises. **L'agence déploie un réseau de correspondants** afin de développer ses actions d'information et de conseil. Toutes les régions métropolitaines sont dotées d'un référent.

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

La mise en œuvre de moyens techniques plus sophistiqués qui assurent à notre pays une capacité de défense souveraine constitue 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[4], en

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

[2] *En partenariat avec le ministère de l'Éducation nationale, de l'Enseignement supérieur et de la Recherche, le Pôle d'Excellence Cyber, des écoles et des industriels*

[3] *Le 27 octobre, l'association a signé un accord avec l'Agence nationale pour la formation professionnelle des adultes (AFPA) visant à rapprocher la formation professionnelle des enjeux de cybersécurité.*

[4] *Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 31 et suiv, http://www.senat.fr/rap/a17-110-9/a17-110-91.pdf*

étroite concertation avec d'autres 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.

Un des volets remarquable est la délivrance de plusieurs types de labels, qui portent aussi bien sur des produits que sur des prestataires de services dans le domaine des technologies de l'information. Le recours à des produits ou services labellisés est imposé par la voie réglementaire dans certains cas ; il est par ailleurs largement recommandé dans tous les autres cas. La mise en œuvre des différents dispositifs de labellisation représente un engagement significatif pour l'ANSSI, qui y consacre une trentaine d'ETP. Elle suit attentivement le processus de mise en place d'un dispositif européen de certification (voir infra).

Le dispositif de labellisation de l'ANSSI

Certification de produits de sécurité

Le décret n° 2002-535 du 18 avril 2002 permet à l'ANSSI de délivrer, après une évaluation approfondie par un laboratoire privé agréé, des certificats attestant de la conformité d'un produit aux objectifs de sécurité définis par un commanditaire[1]. Au titre de ce schéma de certification, l'ANSSI a délivré, en 2017, 94 certificats (nombre stable par rapport à 2016) selon la méthodologie dite des *Critères Communs*, norme internationale, et 24 au titre de la Certification de sécurité de premier niveau (CSPN), approche complémentaire établie dans un cadre purement national. L'agence poursuit par ailleurs ses efforts de promotion à l'international de la CSPN, avec des résultats encourageants[2].

Qualification de produits et de services

L'ANSSI délivre également des qualifications qui peuvent porter tant sur des produits que sur des prestataires de services et ont la portée d'une recommandation. Elle a publié et mis en application, en mai 2017, un nouveau processus de qualification. Elle poursuit par ailleurs le développement du cadre de qualification de prestataires de services et son extension à de nouveaux types de services : après les prestataires d'audit (PASSI) depuis 2013 et les prestataires de certification ou d'horodatage électronique, le dispositif de qualification concerne aujourd'hui les prestataires d'informatique en nuage (SecNum*cloud*) depuis 2016 ainsi que les prestataires de réponse à incident (PRIS) et de détection d'incident de sécurité (PDIS) depuis 2017.

[1] *Une part conséquente des certificats délivrés par l'ANSSI répond à des besoins de sécurité exprimés par des tiers, par exemple par le secteur bancaire, qui exige la certification, selon les objectifs de sécurité qu'il a lui-même définis, des moyens de paiement électroniques. La certification est limitée en l'état aux seuls produits, mais pourrait se voir étendue aux prestataires de service dans le futur cadre européen actuellement en cours de négociation.*

[2] *L'Allemagne et les Pays-Bas ont ainsi mis en place en 2017 des schémas de certification équivalents et l'établissement d'un accord de reconnaissance mutuelle entre les CSPN française et allemande est envisagé pour le début de l'année 2019.*

Au cours de l'année 2017, l'ANSSI a délivré 25 qualifications de produits et 78 qualifications de prestataires de service[1]. Afin d'améliorer cette lisibilité, elle a lancé, en janvier 2018, la démarche « Visas de sécurité », qui instaure un cadre et des éléments de communication communs à l'ensemble des dispositifs de certification et de qualification.

Initiative européenne pour la mise en place d'un dispositif de certification

La Commission Européenne a publié le 13 septembre 2017 une proposition de règlement intitulée *« Cybersecurity Act »*. qui vise à instaurer un cadre harmonisé de certification de sécurité des produits, services et processus numériques. L'ANSSI et son homologue allemand agissent en faveur d'une telle évolution depuis plusieurs années. L'objectif est double : renforcer la sécurité numérique au sein de l'Union européenne en encourageant un large recours à la certification et lutter contre la fragmentation en créant un véritable marché unique harmonisé des produits, services et processus numériques. A la suite de l'adoption de la position du Conseil et du rapport des eurodéputés sur le projet de règlement, qui ont fait évoluer significativement la position initiale de la Commission, les négociations vont se poursuivre. L'ANSSI maintiendra son investissement et assistera le Conseil, dans cette seconde phase ainsi que les travaux lancés par la Commission via *l'ENISA* (*European Union Agency for Network and Information Security*) pour étudier comment effectuer la transition des schémas de certification actuels vers des schémas relevant du *Cybersecurity Act*.

H. LES RELATIONS INTERNATIONALES

La *RCS* présente la France comme un acteur de référence sur le plan international et un chef de file au sein de l'Union européenne. Cette stratégie d'influence doit conduire à promouvoir le modèle français et à participer activement à la définition de normes cyber au niveau européen et international. Cette stratégie doit être menée au sein de l'Union européenne, de l'Alliance atlantique, de l'ONU et dans les diverses instances multilatérales rattachées mais aussi à travers des coopérations bilatérales privilégiées. Elle préconise de renforcer le dialogue avec nos alliés et partenaires pour prévenir les crises cyber[2].

---

[1] *Elle tient à jour un indicateur LOLF « Taux de réalisation du catalogue objectif des produits de sécurité », en progression régulière, qui représente le taux de couverture par des produits qualifiés de la typologie des produits nécessaires à la satisfaction des besoins de l'administration.* https://www.performance-publique.budget.gouv.fr/sites/performance_publique/files/farandole/ressources/2019/pap/pdf/PAP2019_BG_Direction_action_du_Gouvernement.pdf

[2] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf *page 75 et suiv.*

Elle présente ensuite plusieurs propositions visant à mieux garantir la sécurité et l'autonomie stratégique européenne dans l'espace numérique. Au sein de l'Union européenne, la France cherche à promouvoir un meilleur équilibre entre autonomie stratégique européenne pour la sécurité du numérique et maintien de ses prérogatives souveraines, dans une logique de subsidiarité et de respect des compétences des États en matière de sécurité nationale. Ces objectifs s'appliquent pleinement aux enjeux et se déclinent en trois axes technologique, réglementaire et capacitaire[1].

Dans ce contexte, la France continue à défendre le renforcement de la cyber-résilience de l'espace européen (mise en œuvre de la directive NIS[2], coopération pour le traitement des crises de grande ampleur, cybersécurité des institutions et agences de l'UE, etc.) et à promouvoir une politique industrielle ainsi que la prise en compte de la cyberdéfense au sein de la politique de sécurité et de défense commune (PSDC).

En outre, il apparaît nécessaire de développer la coopération opérationnelle entre les États-membres. Les exercices *CyberEurope*, organisés par l'ENISA[3] depuis 2010, ont permis aux États membres de tester leur collaboration en cas de crise majeure, la coopération opérationnelle en cas d'incidents reste embryonnaire. Elle se structure progressivement depuis le lancement du réseau des *Computer Security Incident Response Teams* (CSIRTs) en 2017.

De nombreux États membres connaissent des difficultés pour développer leurs propres capacités et souhaitent que l'Union joue un rôle accru en appui des États victimes de cyberattaques. Le contexte pourrait conduire à un renforcement des obligations des États membres en matière de partage d'informations et d'établissement d'une capacité opérationnelle supranationale. Compte tenu des enjeux de souveraineté associés, la France considère que les échanges opérationnels doivent se faire sur la base de coopérations volontaires et souhaite éviter l'émergence d'une capacité européenne autonome, redondante et compétente pour intervenir au sein des États en réponse à incident. Elle promeut un approfondissement de la coopération volontaire. Cette démarche[4] s'appuie sur quatre principes : une posture claire sur la répartition des compétences et la préservation de la souveraineté nationale en matière opérationnelle, le renforcement des capacités cyber des États, le développement de la coopération opérationnelle au sein de l'UE, la promotion d'un modèle adapté d'assistance aux Etats en cas d'incident, qui soutiennent un secteur privé de confiance fournissant des services mobilisables en cas de crise.

La Revue propose l'adoption d'un schéma de classement des attaques informatiques[5] et d'une doctrine d'action, et analyse, enfin, les conditions d'une meilleure régulation du cyberespace[6].

En lien avec les ministères compétents, l'ANSSI assure la représentation de la France dans les organisations internationales, le suivi

---

[1] *La politique industrielle de l'Union européenne est un vecteur important pour soutenir les capacités de recherche et de développement de pointe ; voir Revue stratégique p.120 et suiv*

[2] *Voir supra p.*

[3] *Agence européenne chargée de la sécurité des réseaux et de l'information*

[4] *Id : p 164 & 165*

[5] *Préalable à l'adoption d'une doctrine d'action face aux attaques cyber, un schéma de classement des incidents a été établi, présenté dans l'enceinte du C4 et validé lors du COPIL cyber de juin 2018. Intégrant les normes juridiques nationales et internationales, il constituera à la fois un outil d'aide à la décision pour les autorités, un élément fondamental d'une doctrine d'action pour la France et un support favorisant la coopération internationale.*

[6] *id : p.79 à 92*

des négociations en matière de sécurité numérique et l'établissement de partenariats notamment opérationnels avec d'autres pays[1].

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

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 l'ANSSI, qui en sens inverse, assure la direction des systèmes d'information pour l'ensemble.

Toutefois afin de faciliter la gestion et l'administration de l'agence, et dans un contexte de montée en puissance particulièrement rapide, une sous-direction affaires générales a été créée en 2016 au sein de l'agence. **Dans un proche avenir, lorsque l'ANSSI arrivera à maturité, vos rapporteurs estiment qu'il conviendra de lui accorder une plus grande autonomie de gestion.** Pour la mesure de sa performance dans la réalisation de ses activités principales ou critiques, l'agence a développé un dispositif à trois composants[2].

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 ;
- 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.

A ce jour, le CTG administre un parc de 1 800 stations ISIS[3] déployées sur l'ensemble du territoire métropolitain et outre-mer et de 4 013 postes TEOREM[4], répartis dans le monde (dont 3 266 sur le réseau Rimbaud et 152 mobiles). 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

---

[1] *Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 33 et suiv,* http://www.senat.fr/rap/a17-110-9/a17-110-91.pdf

[2] *Avis p 35 et suiv.*

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

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

D'un effectif de référence de 183 emplois[1] (dont 172 militaires) pourvu au 1er septembre 2018 à 92%. 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. Il accompagne l'augmentation d'activité des services de renseignement, ce qui implique une évolution de son format et son organisation.

A. DES MISSIONS EN VOIE DE STABILISATION

Les missions du GIC sont fixées par le décret n° 2016-67 du 29 janvier 2016[2] relatif aux techniques de recueil de renseignement et par des arbitrages du Premier ministre.

Les missions du GIC

- la centralisation du circuit de validation des demandes[3].

- l'exclusivité du pouvoir de réquisition des opérateurs de communication électroniques et des fournisseurs de services de communications sur internet pour la mise en œuvre des techniques de renseignement autorisées. Dans ce cadre, il développe et maintient les logiciels à l'usage des services afin de faciliter l'exploitation des données recueillies, organise la traçabilité et contrôle la mise en œuvre et l'exploitation[4] des techniques de renseignement ;

- la centralisation des données recueillies par les techniques dites «de proximité» opérées par les services de renseignement. Il coordonne les modalités de la centralisation dans les autres entrepôts autorisés[5].

- la sécurisation de l'accès des services aux données recueillies. Le GIC accompagne les services de renseignement et de sécurité pour améliorer l'efficacité du travail de leurs exploitants et leur apporte un soutien technique en veillant à minimiser leurs contraintes administratives. Présent à Paris, en banlieue, en province et outre-mer, il offre aux services des emprises sécurisées depuis lesquelles ils accèdent à distance à ses entrepôts pour y exploiter les données recueillies.

---

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

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

[3] *Avis Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 37 et 38. http://www.senat.fr/rap/a17-110-9/a17-110-91.pdf*

[4] *Avis id p. 38.*

[5] *Avis id p. 38 et 39.*

- la garantie d'un niveau de sécurité élevé pour le transport, le traitement et la conservation des informations[1].

- une mission de conseil auprès du Premier ministre pour la mise en œuvre des techniques de renseignement. Le GIC lui apporte les éléments d'évaluation nécessaires[2]. Il est le correspondant privilégié de l'autorité de contrôle, la CNCTR, et le représentant du Premier ministre devant la formation spécialisée du conseil d'État.

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 qui s'est traduit par la publication des textes réglementaires nécessaires à la définition précise de son statut[3], la révision du statut de l'ensemble de ses personnels[4] achevée en 2016 et l'organisation du soutien administratif et financier par le SGDSN[5].

1. L'accroissement de son activité

Depuis l'entrée en vigueur de la loi de 2015 relative au renseignement la progression de l'activité est considérable. Les avis préalables émis, dont le nombre est égal à celui de demandes reçues et qui est représentatif des autorisations accordées, se répartissent comme indiqué dans le tableau général.

---

[1] *Le GIC a mis en place un centre technique secondaire, qui a vocation à devenir un site de dévolution dans le cadre de son plan de continuité et de reprise.*

[2] *Avis id p. 40 et suiv.*

[3] *Décret du 20 décembre 2016 portant création d'un service à compétence nationale dénommé « groupement interministériel de contrôle », comme le recommandait la délégation parlementaire au renseignement dans son rapport pour 2015 p. 35 http://www.senat.fr/rap/r15-423/r15-4231.pdf*

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

[5] *L'adossement administratif et financier du groupement au SGDSN est effectif depuis la fin de l'année 2016 et fait l'objet d'une convention signée le 15 janvier 2018 :*

- *en matière de ressources humaines : l'employeur organique (SGDSN) signe les contrats et exécute les rémunérations, l'employeur opérationnel (GI) gère les congés, ordonne les missions. Les notations / évaluations sont partagées en fonction des statuts.*
- *en matière de gestion budgétaire et de processus d'achat hors fonds spéciaux : le SGDSN est ordonnateur des crédits de l'UO GIC. Le GIC pilote son budget et exprime ses besoins d'achat. Le SGDSN est autorité adjudicatrice des marchés.*
- *en matière de soutien logistique et immobilier : le SGDSN fournit des prestations au profit du GIC*

Techniques de renseignement (*articles du Code de la sécurité intérieure)*	**Avis préalables rendus**		
	2016	2017	Évolution
Accès aux données de connexion en temps différé (art. L. 851-1) (identifications d'abonnés ou recensement de numéros d'abonnement)	32 066	30 116	- 6,2%
Accès aux données de connexion en temps différé (art. L. 851-1) (autres demandes dont celle de factures détaillées)	15 021	18 512	+23,2%
Géolocalisation en temps réel (art. L. 851-4)	2 426	3 751	+ 54,6%
Interceptions de sécurité (art. L. 852-1 I)	8 137	8 758	+7,6%
Autres techniques de renseignement[1]	9 408	9 295	-1,2%
Ensemble des techniques de renseignement	67 088	70 432	+5%

Source : CNCTR – 2ème Rapport d'activité novembre 2017

Elle est due à l'encadrement de techniques dont l'usage se répand dans les services spécialisés et à l'augmentation de l'activité de lutte contre le terrorisme, priorité affichée depuis les attentats de 2015.

2. Une modernisation accélérée des moyen

Afin d'absorber la charge de travail liée à l'augmentation du nombre de demandes, le GIC a dématérialisé le circuit d'instruction de la plupart des techniques de renseignement[2].

Une rénovation du réseau protégé reliant les centres d'exploitation du GIC situés en province aux entrepôts du GIC a été conduite en 2017. En fin d'année, trois centres sur quatre disposaient de nouveaux serveurs et de nouveaux chiffreurs. Le raccordement au réseau interministériel de l'État permet d'atteindre des débits importants, indispensables au bon fonctionnement des applications du GIC.

En 2017, de nouvelles capacités informatiques ont été installées dans le centre technique secondaire du GIC, pour assurer la résilience des services offerts par le groupement.

Des études et des développements ont été lancés en 2016, en liaison avec les services de sécurité et de renseignement, afin de définir les conditions de collecte et de centralisation du renseignement au GIC. Des modalités propres à chaque technique devant être définies, la réalisation des

[1] *Sont incluses les demandes d'accès aux données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure), celles de mise en œuvre de traitements automatisés sur des données de connexion (article L. 851-3 du code), 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'interception de sécurité par IMSI catcher (II de l'article L. 852-1 du code), celles d'interception de sécurité sur un réseau empruntant exclusivement la voie hertzienne (article L. 852-2 du code), celles de captation de paroles prononcées à titre privé ou celles de captation 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).*

[2] *Depuis début novembre 2016, le circuit des demandes d'autorisation utilise un réseau protégé conçu et déployé par le GIC dans quatre ministères, à Matignon et à la Commission nationale de contrôle des techniques de renseignement (CNCTR).*

systèmes informatiques idoines est progressive. Elle a commencé en 2016 avec la mise en service par le GIC de plateformes de centralisation des données de géolocalisation issues des balises. Les principes de la centralisation des captations sonores et vidéo ont été élaborés par le GIC, en concertation interministérielle, pour une mise en service en 2018. Ces réalisations traduisent une véritable montée en puissance du dispositif technique de contrôle.

S'agissant de l'activité opérationnelle historique du GIC d'interceptions de sécurité, les travaux se poursuivent pour moderniser et adapter en permanence les dispositifs d'accès aux communications en prenant en compte les nouvelles normes techniques. Les logiciels d'exploitation à l'usage des services sont en constante évolution et des outils d'aide à l'exploitation sont étudiés afin d'apporter aux services l'assistance technique indispensable à une bonne analyse des données recueillies.

La dématérialisation de la diffusion sécurisée des résultats de l'exploitation mise en œuvre à titre expérimental en 2016, puis pérennisée, a vocation à être étendue aux directions dont les systèmes d'information sont compatibles avec les règles de protection qui s'imposent.

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 et de ses évolutions[1], mais aussi 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. Chacune de ces modifications a des conséquences fortes et immédiates pour le GIC qui doit faire évoluer ses systèmes informatiques et, au besoin, ses infrastructures[2]. Ceci suppose une progression régulière de ses moyens en personnel et en ressources budgétaires ;

- 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.

---

[1] *En 2016 : la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, ainsi que la loi n° 2016-987 du 21 juillet 2016 prorogeant l'application de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence et portant mesures de renforcement de la lutte antiterroriste. En 2017 et 2018, trois textes législatifs sont intervenus pour modifier des dispositions de ce cadre légal : la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique, loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme et la loi n° 2018-607 du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*

[2] *Avis Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 43 et 44.*

o 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 site sont cependant très en-deçà du besoin exprimé mi-2015 par le GIC[1]. **C'est pourquoi une solution pérenne a été recherchée (voir infra p. 56)**

o Par ailleurs, le GIC ouvre de nouveaux centres d'exploitation pour améliorer le maillage territorial et offrir aux services régionaux de sécurité et de renseignement de nouveaux points d'accès à son réseau sécurisé au bénéfice direct de l'activité opérationnelle (voir infra encadré p. 56).

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 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. Cette évaluation réalisée en 2016 ne préjuge pas de moyens qui seront nécessaires au fonctionnement du nouveau site en cours d'acquisition.

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].

1er semestre 2016	2nd semestre 2016	1er semestre 2017	2nd semestre 2017	1er semestre 2018
512	516	560	448	568

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. Au premier semestre 2018, le nombre des demandes de techniques de renseignement est très nettement reparti à la hausse. Par ailleurs, sur cette période, le GIC a enregistré de nombreux départs et des difficultés de recrutement.

---

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

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

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 **311,3 M€** en AE et **294,9 M€** en CP **et le plafond d'emplois à 1 226 ETPT (1 191 en 2018).**[1]

Comme en 2018, son évolution continue de s'inscrire :

- dans **la montée en puissance de l'ANSSI** et **le maintien des capacités d'action et de coordination des deux directions centrales du SGDSN** tout en réalisant des économies de gestion et des redéploiements internes ;
- dans **le développement des moyens nécessaires au GIC.**

CRÉDITS DU BOP SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2019 (EN MILLIONS D'€)

- **Crédits de titre 2**

Crédits de titre 2 en euros	LFI 2017		Exécution 2017		LFI 2018		PLF 2019	
	AE	CP	AE	CP	AE	CP	AE	CP
crédits hors CAS "Pensions"	66 436 865	66 436 865	63 947 170	63 947 170	72 126 825	72 126 825	78 578 121	78 578 121
crédits du CAS "Pensions"	18 665 287	18 665 287	16 466 327	16 466 327	17 547 850	17 547 850	18 628 676	18 628 676
TOTAL	**85 102 152**	**85 102 152**	**80 413 497**	**80 413 497**	**89 674 675**	**89 674 675**	**97 206 797**	**97 206 797**
dont GIC (CAS "Pensions"+ Hors CAS "Pensions"), crédits du PLF	*10 906 848*	*10 906 848*	*10 420 000*	*10 420 000*	*12 559 129*	*12 559 129*	*13 819 526*	*13 819 526*

- **Crédits de hors titre 2**

Crédits de hors titre 2 en euros	LFI 2017		Exécution 2017 (format LFI)		LFI 2018		PLF 2019	
	AE	CP	AE	CP	AE	CP	AE	CP
Total SGDSN	**195 673 936**	**191 077 440**	**170 597 884**	**166 239 953**	**194 481 402**	**196 205 349**	**214 364 102**	**197 999 923**
dont CTIM	82 312 291	82 749 228	64 000 000	67 900 000	83 576 721	83 576 721	77 306 771	77 306 771
dont GIC	15 607 802	15 607 802	15 834 695	11 953 444	15 568 365	15 580 182	17 068 365	17 080 182
dont opérateurs	15 819 824	15 819 824	15 395 178	15 935 178	15 819 824	15 819 824	15 819 824	15 819 824
dont ANSSI	71 423 636	65 867 595	64 733 490	60 883 767	70 207 010	72 928 872	94 741 985	79 375 720
dont SGDSN transverse	10 510 382	11 032 991	10 634 521	9 567 564	9 309 482	8 299 750	9 427 157	8 417 426

Source : SGDSN / réponse au questionnaire budgétaire

[1] *Le BOP SGDSN recouvre les crédits destinés à l'ensemble SGDSN/ANSSI placé sous l'autorité du Secrétaire général de la défense et de la sécurité nationale et les crédits du GIC placé sous l'autorité opérationnel du Premier ministre et en gestion sous la responsabilité du SGDSN, soit l'ensemble des crédits de l'action 2 à l'exception des Fonds spéciaux dont la gestion est placée sous l'autorité de la DSAF.*

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

A. LES CRÉDITS ET LES EMPLOIS INSCRITS AU BOP SGDSN

S'agissant des effectifs, un schéma d'emplois de +52 ETP (dont +42 pour l'ANSSI, +15 GIC et -5 ETP sur les autres services et directions du SGDSN) a été accordé en PLF 2019 pour l'ensemble du SGDSN (action 2), faisant passer le plafond d'emplois de 1 191 ETPT en LFI 2018 à 1 226 ETPT en PLF 2019.

EFFECTIFS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2019

	LFI 2018		**PLF 2019**	
	ETP (schéma d'emplois)	ETPT	ETP (schéma d'emplois)	ETPT
ANSSI	(+25)*		+42	
CTG				
SGDSN hors ANSSI et CTG			-5	
Total SGDSN	+25	978	+37	998
GIC	+15	213	+15	228
BOP SGDSN	+40	1191	+52	1226

(*) Seuls 8 des 25 recrutements prévus devraient être finalement réalisés sur l'exercice 2018. Le solde (17 ETP) a été décalé sur 2019 et inclus dans les + 42 ETP prévus au PLF 2019).
Source : SGDSN / Réponse au questionnaire budgétaire. Les crédits du titre 2 sont donnés à titre indicatif.

En 2017, l'ANSSI a bénéficié d'un schéma d'emplois de +50 ETP, ce qui lui a permis d'atteindre à la fin de cette année 547 ETP. **L'évolution devait se poursuivre à raison d'une croissance annuelle de 25 ETP entre 2018 et 2022 pour atteindre 675 ETP en fin de période[1].** De fait en raison d'une sous-évaluation des crédits inscrits en titre 2, il n'a pu être procédé qu'à 8 créations de postes. Les 17 postes restant seront pourvus en 2019 et s'ajoutent au 25 ETP dont la création était prévue dans le schéma d'emplois**.**

Il était envisagé de faire évoluer les effectifs du GIC 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[2]. Dans le cadre du PLF 2019, les crédits de masse salariale du GIC s'élèvent à 13,8 M€ contre 12,6 M€ en 2018, soit une évolution de 1,2 M€. Cette augmentation correspond à l'effet des schémas d'emplois 2018 et 2019 sur l'année 2019.

Sous réserve de la consolidation des crédits du titre 2, l'estimation de la masse salariale du SGDSN en 2019 est de 97,2 M€, dont 18,63 M€ sur le CAS Pensions. Cette hausse de 8,3% s'explique essentiellement par[3] :

---

[1] *Au sein de l'action 2, le plafond d'emplois demandé pour 2019 de la sous-action 1 (SGDSN hors GIC) est de 998 ETPT, contre 978 ETPT en 2018.*
[2] *Les effectifs du GIC, qui devaient s'établir à 200 ETP à la fin de 2017 et à 215 à la fin de 2018.*
[3] *Elle conduira à un plafond d'emplois à l'échelle du SGDSN de 1 191 ETPT.*

- le schéma d'emplois de l'ANSSI et du GIC, représentant au total 20 ETPT sur le plafond d'emplois ;
- l'effet report des emplois créés en 2018 (41,7 ETPT) ;
- le resoclage du titre 2 pour tenir compte des difficultés de l'ANSSI et ajuster le niveau des rémunérations en conséquence.

Cette estimation de masse salariale intègre également, au titre des mesures catégorielles nouvelles, 0,46 M€ destiné à la revalorisation du régime indemnitaire des agents de l'ANSSI[1].

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

Le SGDSN, qui devra supprimer 5 ETP en 2019, est devenu la structure de portage d'un ensemble d'entités plus ou moins autonomes qui tant en crédits qu'en effectifs, dépasse largement son « cœur historique ». Dans son précédent rapport[2], votre Commission s'était inquiétée de la diminution des effectifs de la fonction support du SGDSN et estimait qu'il devra, en conséquence, veiller à renforcer cette fonction pour assurer efficacement le pilotage et la coordination de l'ensemble. **Vos rapporteurs estiment que cette situation doit faire l'objet d'une attention vigilante[3]**.

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 2019. En effet, elle doit assurer ses missions habituelles dont la charge est en croissance permanente, notamment en matière de traitement des attaques informatiques, mais de surcroît réaliser de nouvelles missions[4] : mise en œuvre des recommandations de la *RCS*, des dispositions de la LPM 2019-2025 relative à la détection des attaques informatiques, et de la directive européenne NIS sur la sécurité des réseaux des opérateurs essentiels.

Le renforcement des moyens de l'ANSSI restera à l'ordre du jour des prochaines années, compte tenu de la croissance des menaces et des enjeux liés à la numérisation croissante des activités humaines.

---

[1] *Cette revalorisation s'inscrit dans l'esprit de la circulaire du Premier ministre 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 ».

[2] *Sénat n° 110 Tome IX (2017-2018) par MM. Olivier Cadic et Rachel Mazuir p. 52.*

[3] *Pour assurer ce renforcement, deux solutions sont envisageables, 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 du SGDSN.*

[4] *Voir supra p.27 et suiv.*

La croissance des effectifs a d'ores et déjà permis à l'agence de passer de 122 ETP en 2009 à 555 ETP fin 2018. A la fin de l'année 2019, l'agence aurait ainsi compté 597 ETP. Toutefois, seuls 8 des 25 recrutements prévus devraient être réalisés en 2018. En effet, les crédits inscrits au titre 2 se sont avérés insuffisants pour permettre les recrutements nécessaires au remplacement des personnels en fin de contrat et aux créations de postes. La concurrence exacerbée sur le marché du travail pour ces profils d'ingénieur et le nombre limité d'ingénieurs qualifiés sortant du cursus universitaire ou des grandes écoles enchérit le niveau de salaire de recrutement. Le DG de l'ANSSI lors de son audition devant votre Commission[1] indiquait que le remplacement d'un ingénieur recruté il y a six ans, se trouvant en fin de contrat ou souhaitant développer sa carrière professionnelle en dehors de l'ANSSI avait désormais un coût, le salaire moyen de recrutement d'un jeune ingénieur étant plus élevé que celui de son prédécesseur malgré son ancienneté.

Le solde (17 ETP) a été décalé et inclus dans les 42 ETP prévus au PLF 2019. Toutefois, l'ANSSI devra mettre 2 ETP à disposition de l'ARCEP[2].

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 compte tenu du développement des menaces, des enjeux et des missions.

1. L'ANSSI est confrontée à la rareté des profils recherchés

Pour maintenir son expertise au meilleur niveau mondial et la renforcer, l'ANSSI doit pouvoir compter sur des agents compétents et maîtrisant l'état de l'art dans de nombreux métiers spécifiques, la plupart du temps inexistants dans la fonction publique. C'est pourquoi l'effectif de l'ANSSI est composé en très grande majorité d'ingénieurs informatiques, recrutés à 79% sous contrat, d'un âge moyen de 37 ans.

L'agence est confrontée à la rareté des ressources humaines de haut niveau dans certaines spécialités et à la tension générale sur les métiers de l'informatique, particulièrement sensible dans les métiers du numérique et de la sécurité des systèmes d'information. L'accroissement de la menace et

[1] http://www.senat.fr/compte-rendu-commissions/20181001/etr.html#toc8

[2] *Pour permettre à cette autorité administrative indépendante de réaliser le contrôle de la mise en œuvre par l'ANSSI des dispositions des articles L 36-7 12° et L 36-14 du code des postes et des communications électroniques et L 2321-5 du code de la défense introduit par l'article 34 de la LPM 2019-2025 pour renforcer les capacités nationales de détection des attaques informatiques (article 19 du projet de loi). Voir* Rapport n° 476 (2017-2018) de M. Christian Cambon, sur le projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense, p. 156 et suiv. http://www.senat.fr/rap/l17-476/l17-4761.pdf

des enjeux accentue les tensions sur les ressources humaines[1]. Ce constat est largement partagé au niveau interministériel et des travaux ont d'ores et déjà été engagés à ce niveau afin de mettre en place un plan d'action pour attirer et fidéliser les agents exerçant ces métiers[2].

2. Un taux de sortie élevée mais dans la norme

En raison de son volume, de sa jeunesse et de la nature des activités menées, l'effectif de l'ANSSI est régulièrement renouvelé. Le taux de sortie a ainsi atteint 18,7%[3] en 2017, en rapport avec les taux observés par ailleurs dans le secteur d'activité.

Ce taux ne crée pas de difficulté particulière. Il préserve l'expertise de l'agence tout en l'alimentant en jeunes collaborateurs à la pointe des connaissances. Par ailleurs, cette rotation permet aux agents d'enrichir leurs expériences et compétences en dehors de l'agence, dans le secteur privé ou public, avec la possibilité de revenir ultérieurement en son sein.

Cette dynamique est rendue possible par la stabilité de l'encadrement supérieur[4] assuré par des fonctionnaires civils et militaires de haut niveau, en position de détachement. L'encadrement intermédiaire[5] est constitué d'agents contractuels à 70%, dont les deux tiers en contrat à durée indéterminée. Cette structure managériale garantit la stabilité indispensable à la poursuite de ses orientations stratégiques et la continuité de son action.

3. Une politique RH adaptée mais sous contrainte

L'attractivité et la fidélisation du personnel doivent être préservées. Elles reposent en grande partie sur l'image très positive de l'agence et sur la qualité de son encadrement.

---

[1] *Le nombre d'emplois dans le domaine de l'informatique devrait encore progresser au cours des dix prochaines années, à un rythme bien supérieur à celui de l'ensemble des métiers (+1,8%), mais avec des évolutions contrastées selon les familles professionnelles. Ainsi, les techniciens et surtout les ingénieurs de l'informatique devraient continuer à bénéficier de perspectives d'emploi favorables (respectivement +1,1% et +2,3% de créations nettes par an), compte tenu des besoins toujours croissants en fonction d'expertise. Rapport* "Les métiers en 2022"- *France Stratégie- Avril 2015.*

[2] *Cf. La circulaire n°5920 du 21 mars 2017 du Premier ministre donnant mandat au SGMAP/DINSIC et à la DGAFP pour remédier à ces difficultés.*

[3] *93 départs/497 agents au 1er janvier. Le taux de sortie est plus adapté que le taux de rotation dans une entité en croissance (ce dernier inclut les arrivées, par nature plus élevées que les départs et donc fausserait la lisibilité de l'indicateur).*

[4] *Direction, sous-directions.*

[5] *Chefs de divisions, chefs de bureaux et de laboratoires.*

Les efforts mis en œuvre pour recruter et fidéliser

Les agents restent au sein de l'agence si leur rémunération de départ est satisfaisante et si elle évolue en fonction de changements de fonctions notamment, mais aussi de l'appréciation de leurs compétences sur le marché. Cette situation implique de s'appuyer sur un processus de recrutement qui tienne compte du poste à occuper et de la valeur sur le marché des compétences recherchées, au-delà de la situation personnelle des candidats, de l'évolution des salaires et des compétences acquises ou fonctions exercées.

Si des actions peuvent être menées en ce sens par le SGDSN avec le concours de l'ANSSI, d'autres doivent l'être au niveau interministériel. Dans ce contexte, l'ANSSI participe aux travaux sur la gestion de la filière numérique animés par la DINSIC et la DGAFP. Ces travaux ont pour objectif de cartographier d'une part les métiers en tension dans le secteur de l'informatique et d'autre part, les rémunérations des agents dans ces métiers. Sur la base des statistiques ainsi établies, la DINSIC engagera une action avec la direction du budget et les services du contrôleur budgétaire et du comptable ministériel visant à permettre des recrutements qui prennent en compte les spécificités évoquées.

L'ANSSI a adopté une politique de communication très active sur ses actions en matière de recrutement *via* le recours à des vecteurs de recrutement adaptés à l'époque, dont les réseaux sociaux spécialisés.

La fidélisation du personnel passe également par l'accompagnement des agents tout au long de leur passage à l'ANSSI. A cette fin, l'identification précise des postes permettant une mobilité interne, ainsi que la définition des compétences et profils attendus pour y postuler, a été engagée. De surcroît, l'ANSSI met en œuvre une politique de formation individualisée ambitieuse.

Enfin, la situation de plein emploi que connaît ce secteur d'activité provoque une concurrence forte entre les secteurs public et privé. Les entreprises du secteur privé développent des stratégies de séduction des candidats, mettant en avant leurs infrastructures d'accueil, les services proposés et des modalités d'organisation du travail renouvelées. Les implantations actuelles de l'ANSSI arriveront à saturation à moyen terme. Elle travaille en lien avec le SGDSN, la DSAF et la DIE à son implantation immobilière afin de lui permettre de répondre à la croissance planifiée de ses effectifs.

Vos rapporteurs estiment que les problèmes de recrutement rencontrés par l'ANSSI et nombre d'administrations et d'entreprises proviennent de la faiblesse structurelle du vivier de formation initiale au regard des besoins.

Une certaine souplesse doit 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. La circulaire du Premier ministre en date du 21 mars 2017[1] a constitué une avancée importante mais elle semble désormais insuffisante si les crédits de Titre 2 ne tiennent pas compte des évolutions observées sur le marché du travail.

Cette tension sur le marché du travail tire les niveaux de rémunération vers le haut alors même que les administrations publiques

[1] *qui invite notamment chaque employeur à conduire* « une politique indemnitaire permettant de valoriser les métiers numériques et SIC pour fidéliser les compétences rares »

doivent réaliser des économies de gestion, ce qui induit des viscosités certaines pour créer les postes nécessaires et définir les niveaux de rémunérations acceptables. Cette spirale fait figure d'un puit sans fond pour les responsables de la direction du budget.

En conséquence, une politique active de développement de filières de formation en écoles d'ingénieurs et en universités doit impérativement être conduite pour pallier ces déficits. 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, voire même en amont du ministère de l'éducation nationale en intensifiant l'apprentissage du codage informatique à l'école[1]. Il y a désormais urgence compte tenu du temps de formation d'un ingénieur. De ce point de vue, les propositions de la *RCS* restent insuffisantes[2] et ces préoccupations mériteraient un portage politique plus affirmé. La formation est aussi un investissement d'avenir.

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

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

Les effectifs du GIC 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)[3].

	2015	2016	2017	2018	2019	2020
En ETP* au 31/12	132	160	200	215	230	243

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

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.

---

[1] https://www.reseau-canope.fr/savoirscdi/cdi-outil-pedagogique/conduire-des-projets/activites-pluridisciplinaires/lecriture-numerique/lapprentissage-du-codage-a-lecole.html

[2] http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf *page 126 et suiv.*

[3] *Exprimé en ETPT, cela porte le plafond d'emplois à 213 ETPT en LFI 2018 et à 228 en PLF 2019*

Les crédits inscrits dans le PLF 2019 au titre 2 de l'unité opérationnelle GIC s'élèvent à 13,8 M€[1] (12,6 M€ en PLF 2018 et 10,9 en PLF 2017) soit une progression de 10% et devraient atteindre 15,5 M€ en 2020.

Vos rapporteurs ne peuvent que se féliciter de cette adaptation aux besoins en construction budgétaire. Reste cependant à réaliser cet objectif.

Dans le schéma d'emploi du GIC étaient prévus les effectifs qui devaient s'établir à 200 ETP à la fin de 2017 et à 215 à la fin de 2018. **Les retards accumulés en 2017 (10 ETP) n'ont pas pu être comblés en 2018[2]. Ce retard pourrait s'accroître légèrement si le GIC ne parvenait pas à recruter d'ici la fin de l'année pour pourvoir aux 15 créations de postes prévues et au remplacement de 29 départs. Pour 2019, il est prévu 15 créations de postes au-delà du remplacement des départs prévus et du *turn over* non annoncé**. De fait, les contraintes immobilières freinent le rattrapage des emplois non pourvus en 2017 et 2018 dès 2019.

2. La politique des ressources humaines du GIC

La réalisation de cet objectif en 2020 suppose une politique des ressources humaines active obéissant 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 doit désormais, au regard de la multiplication des systèmes informatiques et de ses nouvelles missions, recruter des personnels hautement qualifiés[3], développer de nouvelles compétences, constituer des équipes, élaborer des procédures inédites, et se doter d'une compétence juridique de haut niveau.

Cette évolution est en cours.

a) Une structure fortement évolutive

Une analyse de la structure des effectifs du GIC de 2011 à 2017 montre que :

- la proportion d'agents de catégorie A ou officier est passée de 12 à 34% les catégories B et C baissant à due concurrence ;

---

[1] *Dont 9,451878 M€ de rémunérations d'activité (8,6 en PLF 2018 et 7,4 en PLF 2017), 4,084 de cotisations en contributions sociales y compris les cotisations au CAS Pensions (3,7 en 2018 et 3,3 en 2017) et 0,283 de prestations sociales et allocations diverses (0,29 en 2018 et 0,17 en 2017).*

[2] *Dans son avis sur le PLF 2018, Votre commission estimait que l'un des enjeux importants pour le GIC était la réalisation de son schéma d'emplois et demandait que les emplois non pourvus compte tenu des difficultés intrinsèques aux catégories de personnel recherchées et aux conditions spécifiques d'embauche fassent l'objet d'une mesure de report sur le schéma d'emploi de 2018. Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 52.*

[3] *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.*

• 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%.

b) Des difficultés à recruter

Cette politique se heurte à plusieurs contraintes qui ont freiné les recrutements au cours des deux derniers exercices :

• la **faible notoriété** du GIC ce qui restreint le nombre des personnes susceptibles d'être spontanément intéressées ;

• le **manque de locaux** permettant d'accueillir les nouveaux embauchés. Cette difficulté ne sera résolue qu'avec l'ouverture du nouveau site regroupant tous les personnels chargés d'exploiter le renseignement et une partie des agents du GIC ;

• **les délais d'habilitation**. Les délais d'enquête, de 5 à 6 mois aujourd'hui, ont pu dépasser une année pour les personnes recrutées jusqu'à mi-2017, décourageant certains candidats ;

• l'**absence de candidats fonctionnaires sur certains postes et le niveau des rémunérations offertes** :

o pour le recrutement de personnels de catégories B ou C sur certains postes qualifiés comme étant « administratifs », le GIC peine à trouver des candidats éligibles provenant de la fonction publique ; les seuls candidats présentant un profil adapté proviennent de l'extérieur (contractuels). Or l'embauche d'un contractuel sur ces postes ne peut être autorisée qu'après constat de l'infructuosité de la procédure de recrutement d'un fonctionnaire, ce qui peut prendre plusieurs mois.

o pour le recrutement d'ingénieurs et chefs de projets pour conduire les programmes techniques, essentiellement liés au développement de systèmes d'informations complexes et sécurisés, le GIC rencontre des difficultés, liées d'une part au très faible nombre de fonctionnaires susceptibles de réunir les compétences requises et d'autre part, aux salaires peu attractifs offerts par l'État aux personnes prospectées par rapport aux postes équivalents dans le secteur privé.

c) Des axes de progression

La solution aux problèmes d'attractivité et de fidélisation passe par :

• **une capacité à faire évoluer les rémunérations des agents contractuels en fonction de leurs prises de responsabilités et de leur montée en compétence, selon une politique plus dynamique.** Le GIC partage ces difficultés avec l'ANSSI et la DINSIC dans le périmètre de la mission sous examen et plus largement avec l'ensemble des services de renseignement et des directions des systèmes d'information des ministères. **Cette tension sur le niveau de rémunération sur un marché très concurrentiel est en grande partie la conséquence du déficit du système français d'enseignement de former le nombre d'ingénieurs suffisant pour accompagner la transformation numérique de la société** ;

- la reconnaissance de leur niveau de compétence, en particulier par des changements de catégorie au choix permettant de reclasser à un niveau correspondant à leurs compétences et responsabilités des agents historiques du groupement.
- une amélioration des prestations effectuées au quotidien, tant au profit des agents qu'à celui de la direction. Le renforcement de la fonction RH vise à :
  - mettre en place au niveau du groupement un suivi et une prévision de consommation du titre 2 plus fine, rendue nécessaire par l'évolution de la typologie des agents (augmentation du pourcentage de personnels de catégorie A) ainsi que pour l'efficacité du dialogue de gestion avec le SGDSN, responsable de BOP ;
  - parfaire le suivi des congés et permissions, la gestion du compte épargne temps et le décompte des arrêts maladie, en fournissant à l'encadrement intermédiaire les outils nécessaires pour optimiser l'organisation du travail ;
  - mieux suivre les actions de médecine de prévention et de mettre en place les projets d'amélioration de la sécurité au travail adaptés.
  - des évolutions peuvent également être envisagées, avec le responsable de BOP, sur la répartition des responsabilités dans les actions de recrutement.

Vos rapporteurs estiment que les règles de recrutement des contractuels devraient être assouplies dans certaines situations telles que celle du GIC, 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. Le « rebasage » des crédits de titre 2 ne devra pas être exclu a priori. 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 (LES CRÉDITS HORS TITRE 2 EN PLF 2019)

Le PLF 2019 prévoit l'ouverture de 181,47 M€ d'AE (163,09 M€ en 2018) et de 165,10 M€ de CP (164,80 M€ en 2018) pour l'ensemble SGDSN/ANSSI (hors GIC et subvention aux opérateurs). Cela représente, en CP, **une évolution de l'ordre de 0,2% par rapport à la LFI 2018**. Les crédits ouverts seront essentiellement mobilisés sur le développement de la cyberdéfense et la résilience des communications gouvernementales. **L'écart entre CP et AE est en grande partie imputable aux engagements (15,5 M€) pour le renouvellement du bail de la Tour Mercure (siège de l'ANSSI).**

1. L'ANSSI représente une part importante des crédits hors titre 2

La dotation de l'ANSSI (79,38 M€ en CP et 94,74 M€ en AE) est consolidée par rapport à 2018 (72,94 M€ en CP et 70,21 en AE).

Hors ANSSI, le SGDSN dispose de 85,72 M€ en CP pour 2019, soit une diminution de 6,7% que l'on retrouve atténuée en AE (-5,6%) et s'élèvent à 86,73 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 8,41 M€ en 2019 contre 8,30 M€ en 2018 en CP (+1,3%). Pour le reste, les écarts sont essentiellement la conséquence de l'évolution des crédits consacrés à la poursuite de projets interministériels concourant à la défense et à la sécurité nationale transférés en cours d'exercice vers le ministère de la défense dont l'enveloppe diminue sensiblement et s'établissent à 77,31 M€ en AE et en CP (-7,5%).

2. 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 81,2 M€ d'AE et 66,8 M€ de CP et sont destinés à couvrir principalement les dépenses et les actions suivantes :

- **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 1,5 M€ en AE et en CP ;
- **les communications électroniques sécurisées** (17,6 M€ d'AE et 15,8 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 ;
- **la politique d'expertise scientifique et technique et le développement de produits de sécurité** (8 M€ en AE et 7,1 M€ en CP) ;
- la coordination territoriale, les relations internationales et la politique de sensibilisation de l'ANSSI (2,6 M€ en AE et 2,3 M€ en CP) ;
- **6,5 M€ en AE et CP pour le financement des abonnements du réseau Rimbaud ou de son successeur, l'achat de matériels non-immobilisables, ainsi que le coût de l'hébergement et de l'environnement technique. Ce réseau téléphonique est appelé à être remplacé prochainement ;**
- **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… 6,4 M€ en AE et 8 M€ en CP) ;
- une enveloppe de 5,4 M€ en AE et 4,8 M€ en CP dédiés aux programmes interministériels de lutte contre la menace nucléaire, radiologique, biologique,

chimique et explosive (NRBC-E)[1], ainsi que d'autres programmes liés à la lutte contre l'utilisation malveillante de drones ou au réseau gouvernemental d'alerte. De même, sera prise en charge la réalisation d'exercices nationaux de simulation de gestion de crise afin de garantir la continuité de l'Etat.

- 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) ;
- les autres dépenses de fonctionnement courant sont estimées à 7,0 M€ d'AE et 7,5 M€ de CP et couvriront les frais de mission, de formation, d'action sociale, d'équipement et de mobilier, de documentation ainsi que toutes les dépenses de bureautique non spécifiques.

- **S'agissant des dépenses immobilières** :
  - 23 M€ en AE et 11 M€ en CP seront consacrés aux dépenses immobilières pour les sites de l'Hôtel national des Invalides, de la Tour Mercure et du Fort du Mont-Valérien. Ces crédits recouvrent les loyers, charges, taxes, dépenses d'énergie et de fluides, ainsi que les services aux bâtiments comme la maintenance multi technique, la sécurité, ou le nettoyage. En 2019, seront engagées les trois dernières annuités du bail de la Tour Mercure (fin du bail au 01/01/2022).
  - 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[2].

La présentation de ces dépenses dans le PAP s'appuie désormais sur une nomenclature qui semble à peu près pérenne[3] ; l'observation formulée l'année dernière se trouve satisfaite.

3. Les versements des subventions pour charges de service public des opérateurs

Les subventions pour charges de service public des opérateurs sous tutelle 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€.

---

[1] Ces dépenses sont notamment réalisées au travers de conventions avec le Commissariat à l'énergie atomique (CEA), le Laboratoire central de la préfecture de police de Paris et l'Institut franco-allemand de Saint-Louis.

[2] 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.

[3] Certaines dépenses font l'objet d'un reclassement du titre 5 vers le titre 3 notamment celle réalisées au travers de conventions avec le CEA, La préfecture e Police et l'institut Saint-Louis

4. 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 98,1 M€ d'AE et 95,9 M€ de CP pour 2018, ils ont vocation à financer les projets suivants :

- 11,3 M€ d'AE et 9,5 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 les programmes de « *Chiffrement IP* » et « *Crypsis NG* » : de protection de flux classifiés, véhiculés à travers internet ;

- 9 M€ en AE et 7,6 M€ en CP sont prévus pour financer **l'aménagement des salles serveurs du *data center* de Rosny-sous-Bois**[1] : achat de serveurs, matériel réseau (switches, câbles, etc.) et matériel de sécurité (solutions de sécurité, chiffreurs, etc.). Conformément à la convention conclue avec le ministère de l'intérieur, l'acquisition des équipements informatiques des salles serveurs (baies, câblages, cage de Faraday) n'est pas prise en compte dans le budget mutualisé de l'opération, et est dès lors à la charge de chaque ministre ;

- 6,5 M € en AE et CP pour **le financement des évolutions du réseau Rimbaud ou son successeur**. Ce réseau téléphonique est appelé à être remplacé prochainement ;

- 2,8 M€ en AE et 2,4 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 serviront notamment aux réseaux Horus (visioconférence sécurisée) ainsi que tous les réseaux liés aux communications et liaisons officielles ;

- 2,9 M€ d'AE et 2,8 M€ de CP seront destinés à **l'achat de licences et logiciels spécifiques à l'investigation numérique** ;

- 2,3 M€ en AE et 3,8 M€ en CP sont liés à la poursuite des **travaux immobiliers** déjà engagés. Ils concernent notamment la sécurisation de l'alimentation électrique, dont le remplacement des onduleurs, l'amélioration thermique de l'Hôtel national des Invalides, ainsi que la production de froid centralisée.

---

[1] *Lancé en 2014 avec le ministère de l'intérieur, maître d'ouvrage de l'opération, ce projet doit doter l'agence d'un outil informatique performant et fiable. Après 30 mois de travaux, la réception de l'infrastructure a eu lieu le 31 juillet 2018 et la mise en service est programmée pour le second semestre 2018, après des travaux complémentaires d'installation du matériel informatique. Le site sera pleinement opérationnel à partir de janvier 2019.*
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 financièrement à la réalisation du data center proportionnellement aux surfaces occupées.
Le coût global des travaux dans le cadre du marché s'élève à 29,41 M€ dont 22,13 M€ pour le SGDSN suivant la convention de 2015, ce qui correspond à 75% des travaux communs auxquels s'ajoutent certains travaux spécifiques.

• **Par ailleurs, une dotation de 63,3 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 qui jouent le rôle d'opérateurs techniques ; il n'en est pas le bénéficiaire. Du reste, par cohérence, compte tenu de leur destination ces crédits devraient, comme le sont ceux qu'ils abondent, être sortie de l'enveloppe de calcul de la réserve de précaution.

5. Les dépenses d'intervention

Le SGDSN a prévu une dotation de 4,8 M€ en AE et en CP pour les dépenses suivantes :

• 2,2 M€ en AE et 2,5 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 ainsi qu'au financement de l'observatoire de la filière des industries de sécurité ;

• 2,4 M€ en AE et 2,1 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 Conseil supérieur de la formation et de la recherche stratégique (CSFRS).

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

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			
LFI 2017 exécutée (*)	10,1	10,3****	1,8	12,2	
PLF 2018	12,6	3,4***	12,2***	15,6	
PLF 2019	13,8	7,3	9,8	17,1	

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
(****) Titre 3 : 13,9 en AE Titre 5 : 1,9 en AE

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 2019, le budget HT2 en fonds normaux du GIC, **17 068 365 € en AE et 17 080 182 € en CP** (15 607 802 en PLF 2018) tient compte de l'impact des modifications du cadre légal intervenues en 2017 et 2018, de l'accroissement de l'activité liée à celle des services de renseignement, mais aussi des dépenses pour des travaux immobiliers dans un immeuble en cours d'acquisition. **Sont inscrits en titre 3, 7,26 M€ en AE et 7,27 M€ en CP, et au titre 5, 9,81 M€ en AE et en CP.**

1. Les crédits de fonctionnement

Les crédits de fonctionnement courant 7,3 M€ en AE et CP (4,8 M€ en AE, 3,44 M€ en CP en 2018) ont vocation à financer le fonctionnement et le maintien en conditions opérationnelles des différents systèmes d'information et réseaux existants[1], ainsi que le raccordement au réseau interministériel de l'État. Ces crédits couvrent 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 pour 1,7 M€ en AE et CP (1,4 M€ en AE et 1,1 en CP en 2018).

2. Les crédits d'investissement

Les dépenses d'investissement sont essentiellement consacrées à l'achat de licences d'exploitation pour les systèmes informatiques, au règlement d'études, de prestations à caractère technique, à l'achat d'équipements techniques spécifiques (serveurs, calculateurs, capacités de stockage, *etc.*), et aux dépenses d'infrastructure. La montée en puissance du GIC rend nécessaire 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) ;

[1] *Cela regroupe l'achat de matériels réseaux, de matériels de sécurité (firewalls notamment), de postes de travail et de petits matériels. Cela couvre également l'acquisition de licences et les dépenses pour le maintien en conditions opérationnelles des systèmes d'information*

• l'extension du centre de données, 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 (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 encadrées par la loi de 2015. 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 ;

• les plateformes de développement et de recette. L'hébergement des guichets d'exploitation nécessite des infrastructures immobilières et donc, 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**.

Pour 2019, les dépenses d'investissement prévues sont de 9,8 M€ en AE et CP (10,8 en AE et 12,2 en CP en 2018) et se répartissent en :

• des dépenses pour immobilisations incorporelles pour 5 M€ en AE et CP (6,6 M€ en AE et 6,3 en CP en 2018) qui se rattachent notamment aux projets de sécurisation des systèmes d'information, ainsi qu'aux évolutions du cadre légal depuis 2015 ;

• des dépenses pour immobilisations corporelles à hauteur de de 3,3 M€ en AE et CP (4,3 M€ en AE et 5,9 en CP en 2018) qui concernent notamment la réalisation d'un système de développement et de recette, l'extension des réseaux informatiques et l'équipement d'un data center dans le nouveau site ;

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**. **En 2018, 4 nouveaux centres distants ont été créés**, portant le nombre de centres à plus d'une trentaine. Ces centres utilisent 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, relèvent du GIC. **En 2019, 3 centres seront ouverts**, potentiellement un quatrième et 2 centres seront déménagés.

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 rendant possible leur transmission sous forme numérique aux services bénéficiaires à condition que ceux-ci disposent d'un système d'information homologué au niveau « confidentiel défense ».

• des dépenses liées à des travaux immobiliers réalisés dans l'immeuble en cours d'acquisition pour 1,5 M€ en AE et CP. Les implantations parisiennes actuelles sont, en effet, devenues insuffisantes pour faire face à la croissance des effectifs du GIC et des services qu'il héberge.

C'est pourquoi une solution pérenne a été recherchée en remplacement du second centre parisien, pour regrouper dans un même bâtiment tous les personnels chargés d'exploiter le renseignement et héberger une équipe d'agents du GIC. L'acquisition d'un immeuble devrait aboutir avant la fin de l'année 2018, réalisée sur les crédits du compte d'affectation spéciale « gestion du patrimoine immobilier de l'État ». La majeure partie des aménagements seront financés sur ce même CAS. Le solde sur les crédits du programme 129. L'installation des personnels est attendue pout la mi-2020. Dans l'intervalle, avant l'été 2019 il sera procédé à la mise en place de bâtiments modulaires sur le site principal du GIC afin d'accueillir 35 postes de travail. À l'horizon 2020, des crédits supplémentaires devront être réservés en investissement pour l'aménagement et l'équipement complet de ce site, mais aussi en fonctionnement pour les opérations de déménagement et de sécurisation du site (potentiellement en titre 2 selon l'option qui sera retenue).

III. LES FONDS SPÉCIAUX

Les fonds spéciaux, consacrés au financement de diverses actions liées à la sécurité extérieure et intérieure de l'État s'élèvent à 67,2 M€ en AE et CP dans le PLF 2019[1], un montant identique à celui de 2018.

A. LA GESTION ET LE CONTRÔLE DES FONDS SPÉCIAUX

Depuis la loi de finances pour 2002, les fonds spéciaux inscrits au budget des services du Premier ministre sont consacrés exclusivement à des actions en matière de sécurité intérieure et extérieure de l'État.

La direction des services administratifs et financiers du Premier ministre est chargée d'assurer le versement des fonds spéciaux aux services de renseignement bénéficiaires et au GIC. Depuis 2017, la répartition entre services de renseignement des crédits est établie par le coordonnateur national du renseignement et de la lutte contre le terrorisme (CNRLT)[2].

Ces crédits peuvent être abondés en cours d'années par des crédits ouverts par décret pour dépenses accidentelles et imprévisibles (DDAI) ou par décret de transfert.

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[3], **formation spécialisée au sein de la délégation parlementaire au renseignement (DPR)**.

---

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

[2] *Cette répartition est classifiée et ne peut être communiquée.*

[3] *La CVFS est composée de deux députés et de deux sénateurs, membres de la DPR, 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. Ces travaux sont couverts par le secret de la défense nationale. Depuis 2016, elle publie un rapport public en annexe de celui de cette délégation.*

B. UNE ENVELOPPE DE CRÉDITS STABILISÉE

L'évolution du montant des fonds spéciaux depuis 2015 est indiquée dans le tableau ci-dessous.

Année	LFI (en €)	DDAI (en €)	Décret de transfert (en €)	Réallocation de crédits (en €)	Consommation (en €)
2015	49 477 763	12 247 000	34 000 000	8 722 236	104 446 999
2016	56 794 717	8 000 000	6 000 000	3 843 187	74 637 904
2017	67 151 927	17 200 000	-	2 530 000	86 080 000
2018	67 190 341	6 950 000			
2019*	67 190 341				

*PLF

L'écart entre la prévision et la consommation effective s'explique par les mouvements règlementaires (DDAI et décret de transfert) modifiant les crédits ouverts en cours d'exercice ainsi que de dotations complémentaires provenant du programme 129 (redéploiement de crédits, dégel de la réserve de précaution…)
Source : Réponse au questionnaire parlementaire

Dans ses précédents rapports, la CVFS avait souligné le recours très important à des décrets de dépenses accidentelles et imprévisibles (DDAI) et à des décrets de transfert pour abonder en cours d'année les moyens alloués aux services.

Suivant les observations de la CVFS, l'exécutif a, depuis 2015, pris diverses mesures pour limiter cette pratique[1]. Ces mesures semblent produire leurs effets puisque la part des DDAI et autres décrets de transfert et réallocation de crédits dans les recettes, qui était de 52,6 % en 2015, a été ramenée à 23,9 % en 2016 et 22% en 2017.

Pour autant, dans son rapport sur les crédits de 2016[2], la CVFS observe:

- *que la diminution des DDAI ne s'est pas accompagnée d'une augmentation à due proportion de la dotation initiale en fonds spéciaux, alors même qu'un besoin de financement supplémentaire a été exprimé par les services. Or s'il est admis qu'une part importante des DDAI finançait en réalité des dépenses prévisibles, cela aurait dû se traduire par une hausse équivalente des dotations initiales, ce qui n'a pas été le cas ;*
- *qu'au cours de l'exercice 2016, les services spécialisés de renseignement ont pour la plupart puisé dans leur trésorerie pour satisfaire leurs besoins en fonds spéciaux.*
- *Et qu'*en outre, « *au regard de la trésorerie dégradée des services, la commission recommande d'exclure, par principe, les fonds spéciaux de l'assiette de la réserve de précaution. Le calcul de la réserve de précaution du Programme 129 ne devrait ainsi être effectué que sur les seuls crédits normaux, hors fonds spéciaux* ».

Vos rapporteurs s'associent à ces observations et recommandations.

[1] *Rapport de la délégation parlementaire au renseignement pour 2017* http://www.senat.fr/rap/r17-424/r17-42418.html *p.68*
[2] *Id.*

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).

L'élargissement de leur activité pour s'adapter à des besoins croissants de formation et d'information sur les politiques de défense et de sécurité nationale s'est inscrit dans un contexte de stabilisation des subventions pour charges de service public (SCSP) et des emplois, et de mutualisation de certaines de leurs activités et structures.

Pour 2019, les subventions pour charges de service public et les plafonds d'emploi des deux instituts sont maintenus au niveau des LFI 2017 et de 2018 :

- **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, quatre ans après son adoption, à mettre en place un contrat d'objectifs et de performance comme cela fut le cas au cours des périodes précédentes (2011-2014 et 2014-2017) et c'est le cas pour nombre d'établissements publics. **L'existence d'un tableau de suivi de la mise en œuvre des orientations du plan stratégique dont vos rapporteurs ont pu prendre connaissance ne peut en tenir lieu.** Ces retards laissent supposer l'existence de dysfonctionnements soit dans le fonctionnement administratif de l'Institut,

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

soit dans l'exercice du pilotage des relations avec l'Etat. **Vos rapporteurs attendent donc de la nouvelle direction de l'Institut et de la nouvelle SGDSN une remise en mouvement de la démarche stratégique et de façon concomitante la conclusion d'un contrat d'objectifs et de performance comprenant les indicateurs pertinents.**

2. Les activités de l'IHEDN

Selon le rapport d'activité de l'Institut, l'année 2017 a vu un accroissement de 4,4% du nombre de journées de formation/auditeurs-participants qui passe de 26 334 en 2015 à 26 593.

Les formations stricto sensu représentent près de 87,5% de l'activité. Les formations au niveau national constituent 78%: les sessions nationales (*politique de défense, armement et économie de défense, enjeux maritimes*) 38,7%, les séminaires jeunes plus de 16% et les sessions en région près de 17,6%.

Au niveau national, la session *politique de défense* connaît une baisse sensible de 11%[1]. La création d'une session « *Enjeux et stratégies maritimes* » connaît un certain succès (+66,6%)[2]. En revanche, les sessions « jeunes » et en région progressent[3]. Un effort a été produit sur les journées d'information. L'année 2018 s'est inscrite dans la continuité de 2017 avec la reconduction des activités de formation et d'information et quelques formations nouvelles à l'instar de la session nationale « souveraineté numérique et cybersécurité » construite avec l'INHESJ.

La mutualisation avec l'INHESJ initiée en 2011 s'est poursuivie[4].

Si **le rapport d'activité de l'IHEDN[5]** 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).

Vos rapporteurs constatent une nouvelle fois que le rapport annuel continue à présenter des statistiques par journée et ne met pas en rapport ces éléments « physiques » avec les données comptables. Ils demanderont à l'IHEDN dans leur prochain questionnaire parlementaire, une présentation des données sous le format présenté par l'INHESJ.

---

[1] *6848 journées de formation/auditeurs-participants en 2016, 6067 en 2017*
[2] *818 journées de formation/auditeurs-participants en 2016, 1363 en 2017*
[3] *3963 journées de formation/auditeurs-participants aux cycles jeunes en 2016, 4478 en 2017 ; 4500 journées de formation/auditeurs-participants aux sessions en région en 2016,4878 en 2017*
[4] *voir infra p.70*
[5] *https://www.ihedn.fr/sites/default/files/atoms/files/le-rapport-activite-2017-de-ihedn.pdf*

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.

Les effectifs de l'IHEDN ont été réduits de 12 ETP entre 2014 et 2018 et la subvention pour charges de service public a été réduite de 8,8 M€ en 2012 à 7,6 M€ en 2018, soit une baisse de 13,6%. Pour autant, le budget global est resté stable, autour de 10,3 M€ grâce à une augmentation constante des recettes propres qui atteignent 2,7 M€ en 2018.

En 2017 la part des subventions représente 72,4% des produits (sensiblement moins qu'en 2016 77,4%). La part des ressources propres atteint 22,2% et financement de l'Etat fléchés 4,8% et la taxe d'apprentissage 0,5%. Les charges de personnel représentent 70% des dépenses.

Le montant de la subvention annoncée pour 2018 après régulation est de 7,5 M€. Le nombre d'ETPT autorisé reste de 92. Trois autres emplois en fonction au sein de l'IHEDN restent rémunérés par d'autres programmes en LFI 2018[1]. 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. **On peut s'interroger sur les conditions de cette mise à disposition qui ne permet pas une appréciation du coût réel des charges de personnel de l'institut.**

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. Pour autant, la progression de 14,7% des recettes propres a permis de compenser la baisse de la subvention (-2,28%) et celles des recettes de la taxe d'apprentissage (-23,24%) et de dégager un excèdent de 0,8 M€. **L'IHEDN a donc au cours de cet exercice réussi à développer ses activités, à faire progresser ses recettes extérieures** (droits d'inscription, partenariats, mécénats) et à maîtriser ses dépenses**. L'IHEDN est donc entré dans une phase de stabilisation de sa trajectoire financière, en répondant aux exigences de sincérité et de soutenabilité.**

L'exercice 2019, en maintenant subvention et plafond d'emplois au niveau de 2018, représente une opportunité de consolidation dans la gestion de l'Institut.

Vos rapporteurs estiment que désormais l'IHEDN devrait reprendre une démarche stratégique conjointe avec l'INHESJ pour rationaliser l'offre de prestations et poursuivre la mutualisation des soutiens. Cette démarche devrait constituer la base d'un nouveau plan stratégique et d'un contrat d'objectifs et de performance entre l'Etat et l'établissement.

[1] *Comme en PLF 2019*

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. Il devra mettre en place une offre plus dynamique de formation pour dégager des ressources nouvelles et optimiser les formations existantes.

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

Opérateur public de référence dans les domaines de la formation et de la recherche liés à la sécurité globale et à la justice, l'INHESJ prépare les cadres des secteurs publics et privés à l'exercice de leurs responsabilités et accueille également l'Observatoire national de la délinquance et des réponses pénales (ONDRP) qui est l'un de ses départements[1].

A. MISSIONS ET ACTIVITÉS DE L'INHESJ

1. Les missions formalisées dans un plan stratégique

Le nouveau plan stratégique 2018-2021[2] comporte quatre axes stratégiques, déclinés en objectifs opérationnels, donnant lieu à l'établissement de feuilles de route d'actions précises et intègre les objectifs partagés de mutualisation avec l'IHEDN.

Présentation plan stratégique 2018-2020

Axe 1 : Face à une menace globalisée, faire de la dimension interministérielle de l'INHESJ un puissant levier d'action au service des décideurs publics et privés.
Construire avec les ministères de référence, de l'Intérieur et de la Justice les conditions d'une offre de formation et d'études à la hauteur des enjeux contemporains.
Faire de l'institut une structure de formation de référence pour tous les services de l'Etat comme pour le secteur privé.
Au-delà de la mission de formation, intensifier les coopérations de l'Institut avec tous les ministères concernés.
Valoriser la place et l'activité interministérielle de l'institut pour dynamiser les échanges avec les représentants des entreprises et des industries de la sécurité privée.

[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.*
[2] *Adopté par le conseil d'administration du 29 novembre 2017 et signé par le secrétaire général à la défense et la sécurité nationale et la directrice de l'INHESJ le 21 février 2018*
https://inhesj.fr/sites/default/files/inhesj_files/telechargements/Plan_strat%C3%A9gique_2018-2021.pdf

Axe 2 : Soutenir une ambition prospective forte pour contribuer à l'émergence de politiques publiques adaptées aux nouveaux enjeux de sécurité et de justice.
Structurer les relations de l'INHESJ avec l'université.
Agréger autour de l'institut un réseau diversifié d'experts et de décideurs publics et privés.
Organiser les conditions de rencontres génératrices de connaissances nouvelles entre chercheurs et professionnels de la sécurité et de la justice.
Construire une programmation de colloques et de séminaires à forte teneur prospective.

Axe 3 : Amplifier le rayonnement de l'INHESJ pour diffuser un « esprit de sécurité et de justice ».
Valoriser les études et recherches conduites à l'INHESJ.
Contribuer à la conception de politiques publiques et aider à leur accompagnement au profit de décideurs publics et privés.
Mieux ancrer l'institut dans le paysage national.
Ancrer l'institut dans le paysage international.

Axe 4 : Assurer le plein déploiement du projet stratégique de l'INHESJ en consolidant son administration générale et dynamisant son modèle économique.
Valoriser le parcours des personnels de l'INHESJ par une politique de gestion des ressources humaines active.
Dynamiser le modèle économique de l'institut en développant sa capacité de recours aux financements du secteur privé.

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

Afin de traduire et conforter **les orientations du nouveau Plan stratégique,** un nouveau contrat d'objectifs et de performance (COP) **entre l'INHESJ et l'Etat** a été présenté et signé **en même temps que ce dernier.** L'ensemble des orientations du plan stratégique est complété par 41 indicateurs de suivi avec indication d'une cible à atteindre. Vos rapporteurs ont reçu communication des premiers résultats, mais il est prématuré d'en tirer des conclusions**.**

Vos rapporteurs saluent cette initiative qui répond aux observations formulées par la Commission dans un précédent rapport[1] 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.

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.

[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.90*

a) Les activités de formation

En 2017, l'INHESJ a délivré 2 317 heures de formation (2 297 en 2016) au profit de 2 201 auditeurs et stagiaires (1 719 en 2016). 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 2017 à 81 196 (68 456 en 2016) et pour 12 030 journées stagiaires[1] dont 5 462 pour le département formation « *sécurité police* », 2 284 pour le département « *intelligence et sécurité économique* » et 4 284 pour le département « *risques et crises* », indicateur utile pour suivre l'utilisation des locaux, (7 574 en 2016).

D'un point de vue qualitatif, l'indicateur de satisfaction des auditeurs et stagiaires s'est globalement maintenu en 2017. La moyenne des 3 sessions nationales passant de 3,49 à 3,44 (3,08 en 2015), 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, notamment en répondant à des appels d'offre publics. Les formations représentent 96% des ressources propres. Une de ses caractéristiques est de délivrer des formations diplômantes.

L'ambition de l'institut pour les sessions nationales de formation 2017/2018 a été de mettre en place une méthode pédagogique innovante en associant à la construction de la programmation les ministères de l'intérieur et de la justice et leurs principales directions. Le but était de construire une offre de formation de haut niveau répondant aux préoccupations des administrations confiant des auditeurs[2].

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.

Les études et les recherches sont conduites essentiellement par deux départements :

- le département « *Etudes et recherches* » composé de cinq chercheurs et organisé autour de trois axes particulièrement pertinents au regard des menaces et défis actuels : l'analyse des activités des organisations criminelles et des circuits financiers afférents, la recherche sur la prévention de la radicalisation[3] et l'analyse des modèles de police.

---

[1] *Nombre donnés par le rapport annuel d'activité 2017 p.2 le suivi des indicateurs du plan stratégique indique 11 050 dont 4482 pour le département formation sécurité police*

[2] *INHESJ rapport d'activités 2017 p. 6 à 11*
https://inhesj.fr/sites/default/files/RA_2017_INHESJ_2017ok.pdf

[3] *L'INHESJ assure le secrétariat général du Conseil scientifique sur les processus de radicalisation. 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*

- l'observatoire national de la délinquance et des réponses pénales (ONDRP). Chargé depuis plus de dix ans de produire des analyses sur l'évolution des phénomènes criminels, les caractéristiques des auteurs et des victimes, il nourrit le débat démocratique grâce à sa méthodologie reconnue, sa production et son exploitation de données fiables et objectives sur les sujets de sécurité et de justice.

L'institut souhaite ancrer la prospective au sein de l'ensemble de ses activités, qu'elles soient de formation ou de recherches. Il s'agit d'impulser une démarche de transfert de connaissances, entre chercheurs et acteurs opérationnels. A cette fin une nouvelle direction chargée des relations publiques et de la prospective a été créée, avec l'ambition d'agréger autour de l'institut un réseau diversifié d'experts et de décideurs publics et privés.

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

1. Un développement financé par la croissance des ressources propres

La réduction d'un cinquième puis la stabilisation du montant de la subvention pour charges de service public depuis 2017 à 6,2 M€ en AE comme en CP ont contraint l'INHESJ à rechercher une valorisation de ses prestations. La stabilité sur la durée du COP lui assure un socle pour son développement, une solution bien préférable aux coupes budgétaires annuelles décidées au dernier moment et qui doit être maintenue.

La baisse de la subvention en 2017 a pu être compensée par une hausse de 8% des ressources propres[1], lesquelles atteignent 1,34 M€ en 2017 et devraient atteindre 1,89 M€ en 2018. Cette augmentation repose sur des projets identifiés dont la mise en œuvre a été, depuis lors, largement engagée. L'attention va être portée sur la pérennisation de certaines recettes sur plusieurs années, comme cela est prévu dans le contrat d'objectifs et de performance.

L'optimisation des formations existantes grâce aux recrutements d'auditeurs en provenance du secteur privé et la création de nouvelles formations courtes et ponctuelles y contribueront. Cet effort d'innovation pédagogique impliquera des redéploiements d'effectifs entre les départements. Le conventionnement avec certains des partenaires récurrents permettrait d'améliorer la visibilité budgétaire en pérennisant certaines recettes sur plusieurs années.

Enfin, au-delà des revenus tirés directement des prestations réalisées, le développement de l'Institut passera par sa capacité à s'associer

[1] *Les ressources propres (1,342 M€ en 2017, 1,890 M€ prévue en 2018) sont constituées à 96% 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.*

avec des partenaires privés apportant une contribution financière aux objectifs qu'il poursuit, par la voie d'un fonds de dotation d'un montant de l'ordre de 0,3 M€. Ce fonds pourra ainsi contribuer à soutenir des jeunes chercheurs dans leurs travaux sur des sujets à l'intersection des enjeux de sécurité et de justice ou à la création d'une chaire.

2. Des effectifs plafonnés et maîtrise de la progression de la masse salariale

Pour 2019, le plafond d'emplois est maintenu au même niveau de 73 ETPT[1] qu'en 2017 et 2018. En 2016, le nombre d'ETPT consommés a été de 61,29 et a pu être remonté à 63,62 en 2017. La prévision de consommation d'ETPT pour l'année 2018 est de 65,8 ETPT.

Avec des effectifs réduits de 8 ETP entre 2014 et 2017, l'INHESJ a également procédé à un « dépyramidage » des postes, ce qui lui a permis de contenir sa masse salariale[2], par des recrutements ciblés et moins coûteux (jeunes chercheurs spécialisés, par exemple).

Celle-ci progresse néanmoins 4,96 M€ en 2017 (contre 4,89 en 2016) et 5,3 M€ dans le budget 2018. Cette progression résulte pour une large part du développement de l'activité et doit être mise en regard de la progression des ressources propres.

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 la retenue observée par le contrôle budgétaire sur des recrutements nouveaux bien que l'INHESJ n'atteigne pas le plafond d'emplois autorisé ce qui ne permet guère de lancer la préparation et la réalisation de ces actions. Vos rapporteurs estiment qu'une plus grande souplesse en ce domaine serait utile d'autant que la politique de maîtrise de dépenses par la nouvelle direction de l'institut commence à porter des fruits.

3. Une politique de maîtrise des dépenses publiques

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

---

[1] *auxquels s'ajoutent 5 emplois rémunérés par l'État par d'autres programmes (dont le directeur, un préfet, des personnels des ministères de la justice, de l'agriculture, de l'économie et des finances) ainsi que deux emplois rémunérés par les collectivités territoriales (officiers de sapeurs-pompiers) mis à disposition contre remboursement.*

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

du fonctionnement. Les dépenses de fonctionnements sont passées de 2,6 à 2,5 M €[1].

Le montant des dépenses d'investissement s'est stabilisé à hauteur de 0,2 M€ après un exercice 2016 à 0,76 M€ en raison de la création du plateau de gestion de crise.

La situation immobilière se limite, à compter de 2017, à l'occupation d'une partie du bâtiment 13 de l'École militaire (voir infra p.67).

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[2] pour répondre aux nouveaux besoins de formation dans ses domaines de compétence. L'enjeu sera également de pérenniser une part plus importante des ressources propres.

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.

La synergie des fonctions administratives est accentuée :

- la mutualisation de la fonction « Achats » est largement avancée avec le rattachement progressif des instituts aux accords-cadres interministériels ou ministériels d'achats courants proposés par le Service des Achats de l'Etat et les Services du Premier ministre ;

- la mise en place d'agence comptable unique depuis 2016. En 2017 une démarche commune en matière d'inventaire tant physique que comptable a été lancée. Une réflexion est entamée sur la création d'un service facturier commun. Un aboutissement est recherché pour le 1er janvier 2020.

- en matière de ressources humaines, les outils sont partagés. Les deux Instituts disposent du même outil de gestion des rémunérations. Les projets concernent : l'amélioration et l'élargissement du logiciel commun pour en faire un outil complet ; une politique conjointe de formation pour les agents des deux instituts ; et une meilleure coordination des calendriers. Pour autant, les deux instituts considèrent que le pilotage de leur politique RH constitue une activité de direction qui ne peut être mutualisée.

[1] *En 2017, des économies ont été réalisées sur les voyages d'études, sur les prestations réalisées pour le compte du ministère de l'Europe et des affaires étrangères, les télécommunications et les dépenses de réceptions, à hauteur de 0,09 M€.*

[2] *En 2017, le nombre de jours de formations (226) au profit de 38 bénéficiaires a plus que doublé.*

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

Concernant les outils informatiques : l'intégration des réseaux et serveurs est réalisée, le partage ou le choix en commun de logiciels se poursuit, de plus, l'effort s'est concentré sur la réduction des coûts de fonctionnement liés à l'Internet tout en augmentant le confort et la sécurité. L'année 2018 devra permettre une consolidation des solutions matérielles mutualisées, l'entraide des équipes informatiques ainsi que la poursuite de cet effort en matière d'équipement et de solutions logicielles.

Synergie des pôles de formation.

Les différents pôles formation des deux Instituts se coordonnent régulièrement sur leurs contenus et intervenants, afin d'offrir un enseignement cohérent et pertinent. Au sein de leurs sessions nationales, l'INHESJ et l'IHEDN organisent plusieurs journées communes. Les deux instituts expérimentent de nouvelles modalités de rapprochement. En 2018, ce processus a abouti à la matérialisation de la nouvelle session « *Souveraineté numérique et cyber-sécurité* ». La complémentarité des formations en intelligence économique a été mise en place en 2015. Enfin, une coopération sur la session « jeunes » devrait être expérimentée prochainement.

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, il serait souhaitable de faire converger davantage les démarches stratégiques et contractuelles des deux Instituts, notamment 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**[1].

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 2019 ; les sénateurs du groupe CRCE s'abstenant.

[1] *Les éléments figurant dans le rapport annuel de l'INHESJ constituent une base minimale utile. Vos rapporteurs engagent l'IHEDN à la reprendre dès 2019.*

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 7 novembre 2018.

M. Christian Cambon, président. - Nous commençons aujourd'hui l'examen des avis sur les crédits des différentes missions dans le projet de loi de finances pour 2019 par ceux du programme 129 de la mission « Direction de l'action du Gouvernement ».

M. Rachel Mazuir, co-président du programme 129. - Comme chaque année, nous allons présenter notre avis sur les crédits de l'action 2 du programme 129. Cette action représente plus de 52% des crédits de ce programme.

Dans un budget marqué par la volonté de réduire la dépense publique, cette action, il faut le souligner, progresse. Elle est dotée de 378 millions d'euros en AE (+7,7%) et de 362 en CP (+ 2,4%). C'est, pour l'essentiel, la conséquence de la montée en puissance du Groupement interministériel de contrôle (GIC), et de l'Agence nationale de sécurité des systèmes d'information (ANSSI), dont vous parlera Olivier Cadic.

S'agissant du cœur historique du Secrétariat général de la défense et de la sécurité nationale (SGDSN), Mme Landais nous a exposé, le 3 octobre, la diversité de ses missions. Je voudrais formuler deux observations :

Première observation : nous constatons une intensification de l'activité, signe d'une aggravation des menaces. Pour illustrer ce propos, je relève que le rythme des réunions du Conseil de défense et de sécurité nationale reste toujours soutenu (45 réunions entre le 1er novembre 2017 et le 1er octobre 2018).

Premier exemple : la publication de la première Revue stratégique de cyberdéfense en février 2018, aboutissement d'un important travail interministériel de réflexion et de consultation. Elle dresse un panorama de la cybermenace. Elle trace le cadre doctrinal et d'organisation de la cyberdéfense française et s'attache à consolider le modèle français, fondé sur la séparation des fonctions offensives et défensives, ces dernières assurées, au premier chef, par l'ANSSI. Elle appelle à la mise en place de quatre chaînes opérationnelles : protection, action militaire, renseignement et investigation judiciaire. Enfin, la Revue met en avant le concept de souveraineté numérique, entendu à la fois comme le fait de conserver une capacité autonome d'appréciation, d'action et de décision dans ce domaine, et de protéger les autres composantes de la souveraineté nationale des menaces engendrées par la numérisation. Cette souveraineté doit reposer, notamment, sur la maîtrise de certaines technologies-clefs et sur la consolidation d'une base industrielle nationale ou européenne.

Deuxième exemple : je choisis à dessein des sujets d'actualité, le contrôle des exportations de matériel de guerre, pour vous livrer quelques statistiques sans entrer sur le fond des dossiers. Sur la période d'août 2017 à août 2018, la commission interministérielle pour l'étude des exportations de matériels de guerre, qui donne un avis au Premier ministre pour l'obtention des licences d'exportation, s'est prononcée sur 6 326 dossiers dont 5 062 nouvelles « demandes de licence ». Environ 92 % des demandes ont fait l'objet d'un traitement en procédure « continue » avec avis favorable. 58 % des demandes ont été accordées avec des conditions particulières d'encadrement. La Commission s'est réunie en session plénière à 11 reprises pour l'examen de 517 nouveaux dossiers, soit deux fois plus que sur la précédente période de douze mois, pour lesquels elle a prononcé 388 avis favorables et 117 avis défavorables.

Enfin, dernier exemple, la poursuite des déclinaisons du plan VIGIPIRATE avec la finalisation d'un plan gouvernemental « Pirate Mobilités terrestres » de réaction à un acte terroriste dans ce domaine.

Deuxième observation : 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 qui, en crédits comme en effectifs, dépasse largement le cœur historique du SGDSN.

Si les entités rattachées ont vu leurs moyens croître, tel n'a pas été le cas depuis plusieurs années du SGDSN stricto sensu qui a perdu 25 emplois depuis 2009 avec, pour conséquence, un affaiblissement de la fonction « soutien ». Les effectifs du SGDSN stricto sensu devraient être réduits de 5 emplois dans le PLF 2019, mais les crédits hors titre 2 (8,4 M€ contre 8,3 M€ en 2018) sont maintenus.

Ma seconde série d'observations concerne le GIC qui, dans le cadre de la loi relative au renseignement de 2015, est le pivot interministériel de gestion de l'ensemble des techniques sur autorisation du Premier ministre et sous le contrôle de la CNCTR. L'évolution des menaces a entraîné une intensification de son activité, et des modifications fréquentes du cadre légal. En conséquence, le GIC a adapté ses structures et son organisation. Il a réalisé un certain nombre d'investissements portant sur ses systèmes informatiques et ses infrastructures.

Il disposera, fin 2018, de 215 ETP, 243 à l'horizon 2020. En 2019, 15 emplois devraient être créés. Toutefois, le Groupement s'est heurté à des difficultés de recrutement liées :

- à la transformation progressive de sa structure d'effectifs ;

- à la faiblesse du vivier et à la vive concurrence dans certaines spécialités informatiques et donc à l'évaluation insuffisante des crédits de titre 2 en LFI 2018 ;

- à l'allongement de la durée d'instruction des demandes d'habilitation qui décourage certains candidats ;

- et à des conditions d'hébergement insuffisantes pour faire face à la progression des effectifs.

Un effort budgétaire est réalisé pour accompagner sa montée en puissance. Les crédits de titre 2, réévalués, progressent de 10 % et atteignent 13,8 M€ dans le PLF 2019. Les crédits hors titre 2 stabilisés à 15,6 M€ en 2018, s'élèveront à 17,1 M€ en AE et en CP dans le PLF 2019 (+9,6 %). Ils permettront d'assurer le fonctionnement courant et le maintien en condition opérationnelle des différents systèmes d'information et réseaux et celui de la structure, mais aussi l'achat des équipements nécessaires au développement de son activité, et, notamment, pour le nouveau site en cours d'acquisition qui devrait être opérationnel en 2020. L'acquisition et les aménagements immobiliers seront financés par le Compte d'affectation spéciale « Gestion du patrimoine immobilier de l'Etat ». Cet immeuble permettra de regrouper tous les personnels chargés d'exploiter le renseignement en région parisienne et une partie des agents du GIC, les implantations actuelles étant devenues insuffisantes. Le Groupement devra se montrer vigilant pour évaluer les charges nouvelles que représentera le transfert d'une partie de son activité d'un immeuble accueillant d'autres structures, et hautement sécurisé, à un immeuble nouveau complètement dédié.

Quelques mots sur les fonds spéciaux. L'enveloppe est maintenue à son niveau de 2018, 67,4 M€.

Enfin, j'en viens aux deux opérateurs, l'IHEDN et l'INHESJ. Comme en 2018, le maintien en 2019 des crédits et plafonds d'emploi - 7,6 M€ et 92 ETPT pour l'IHEDN, 6,2 M€ et 73 ETPT pour l'INHESJ - apporte de la stabilité à ces établissements et doit leur permettre de développer leurs ressources propres. L'INHESJ a adopté un nouveau plan stratégique et contracté concomitamment avec l'Etat un contrat d'objectifs et de moyens. Cette démarche incomplètement menée dans la période précédente par l'IHEDN doit être entreprise, à notre sens, sans délai, par le nouveau directeur. Cet institut devra également se doter d'indicateurs de suivi et de performance plus pertinents. Enfin, les deux établissements sont

invités à s'engager plus avant dans le processus de mutualisation des fonctions de soutien et au-delà à développer des synergies pour rationaliser leur offre de formation. L'ouverture, cet automne, d'un cycle commun dans le domaine de la cybersécurité est un bon exemple à poursuivre.

M. Olivier Cadic, co-rapporteur du programme 129. - Je m'associe aux propos de Rachel Mazuir et formulerai pour ma part quelques observations concernant l'ANSSI.

La cyberdéfense est un enjeu majeur. Les menaces sont croissantes, multiples et plus sophistiquées. Elles évoluent à raison de la puissance et de la virulence des réseaux criminels qui investissent le cyberespace à la recherche de gains massifs à moindre risque et par l'action d'autres acteurs, notamment étatiques qui se livrent à des actions d'espionnage, d'ingérence, de sabotage et de déstabilisation. On l'a vu encore récemment avec une affaire d'espionnage russe aux Pays-Bas. Elles évoluent, également à raison de l'accroissement des enjeux dans un monde de plus en plus connecté, et donc de plus en plus vulnérable. Le rapport « Symantec 2018 » classe la France au 9e rang des pays où la cybercriminalité est la plus active et détaille les nouvelles tendances comme des détournements de puissantes machines pour générer de la cryptomonnaie, la banalisation des demandes de rançons, ou et l'injection de programmes malveillants au sein de logiciels légitimes. On assiste même sur le « dark web » à l'émergence d'un marché d'outils informatiques offensifs sophistiqués, porteurs de vulnérabilités. L'attaque NotPetya, en juin 2017, qui a démarré en Ukraine et qui a touché en France le groupe Saint-Gobain en est un parfait exemple. Idem pour la vague d'attaques par le rançongiciel Wannacry en mai 2017 qui a impacté près de 250 000 entités dans plus de 150 pays.

Cette menace est prise en compte depuis une dizaine d'années par l'Etat avec la création de l'ANSSI en 2009. La LPM de 2013 lui a confié de nouvelles missions en matière de protection des systèmes d'information des opérateurs d'importance vitale. Ce champ de compétences a été étendu en 2018 suivant les conclusions de la Revue stratégique de cyberdéfense, ainsi que par les dispositions de la LPM 2019-2025 que nous avons votées cet été et celles issues de la transposition de la directive NIS.

Pour conduire cette politique, l'ANSSI voit ses moyens progresser en 2019 :

Ses effectifs passeront de 555 à 595 ETP, + 40. 25 emplois au titre de son schéma initial et 17 emplois qui auraient dû être créés en 2018, que l'Agence n'a pas été en mesure de financer en raison de la sous-évaluation des crédits de Titre 2. En effet, avec un turn over supérieur à 15 % de son effectif, c'est une petite centaine de collaborateurs que doit recruter l'ANSSI et le montant des rémunérations demandées à l'embauche par les jeunes ingénieurs excède désormais celui des cadres dont ils assurent le remplacement. Ces tensions sur un marché très concurrentiel ont conduit également à un rebasage de la masse salariale qui se traduit par un accroissement des crédits du titre 2 du SGDSN de 8 % qui passe (hors GIC) de 77,1 M€ à 83,4 M€. Deux emplois seront transférés à l'ARCEP en 2019 au titre du contrôle en application des dispositions votées en LPM 2019-2025.

Hors titre 2, et pour la seule ANSSI, les crédits passent de 72,9 M€ à 79,4 M€ en CP (+8,8 %) et de 70,2 à 94,7 M€ (+35 %) en AE. L'écart est largement dû à l'engagement des trois dernières annuités du bail de la tour Mercure où l'ANSSI est installée.

Les principales opérations concernent le financement direct de l'aménagement des salles serveurs du data center, construit en partenariat avec le ministère de l'intérieur, l'engagement de crédits pour le financement du réseau Rimbaud des communications de l'Etat ou de son successeur, le développement de produits de sécurité pour la protection des informations classifiées dans le cadre de programmes conjoints avec le ministère des armées et le fonctionnement des systèmes d'information sécurisés.

Nous sommes satisfaits de cette évolution des crédits de l'ANSSI. Pour autant, nous devons vous faire part de notre inquiétude et relever quelques points de vulnérabilité :

- Le premier concerne le retard persistant de mise en œuvre de la Politique de sécurité des systèmes d'information de l'Etat. 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 d'assurer une détection optimale, explique cela. Les ministères régaliens sont les bons élèves, mais on peut légitimement être inquiet s'agissant des autres ministères. Les entreprises privées sont conscientes de l'obligation pour elles de rehausser leur niveau de sécurité. Ces décisions sont débattues aujourd'hui en comité exécutif dans les grandes entreprises. Le faible portage politique par les ministres et l'insuffisance des capacités d'investissements de la DINSIC et des DSI ministérielles par rapport aux enjeux est assez consternant. Les administrations multiplient les programmes informatiques pour réaliser des économies, mais au détriment, des investissements de cybersécurité, ce qui fragilise la résilience des services publics. Nous lançons un cri d'alarme. Il nous semble nécessaire de poser une règle de principe d'interdiction de développer de nouvelles applications sans investissement conséquent dans le domaine de la sécurité.

- Notre deuxième point de préoccupation, ce sont les problèmes structurels de recrutement et de fidélisation des ingénieurs spécialistes de cybersécurité. Ceux-ci continuent à être très recherchés tant dans le secteur public que dans le secteur privé. L'insuffisance du vivier issu de la formation en école d'ingénieurs ou en université est patente. Ceci induit de fortes tensions sur le marché du travail. Les administrations ne pourront suivre sans un alignement des rémunérations, mais ce sera un puits sans fond sans 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. C'est désormais un enjeu majeur de société qui devrait être porté au plus haut niveau de l'Etat.

- Notre troisième point d'attention est l'importance de la détection en matière de prévention des cyberattaques. Elle doit être réalisée le plus en amont possible. Nous avons, dans la LPM, renforcé les capacités d'action de l'ANSSI. Plus en amont encore, il est souhaitable de mettre en place un véritable réseau de veille au niveau européen, ce qui veut dire une coopération fluide entre Etats disposant d'opérateurs comme l'ANSSI - ils sont rares - et la mise à niveau des Etats qui n'en disposent pas avec l'appui de l'Union européenne.

- Enfin, s'agissant de l'ANSSI, le bail de la Tour Mercure viendra à échéance le 1er janvier 2022, c'est demain. Il faut engager dès maintenant les études pour rechercher une nouvelle implantation qui concilie montée en puissance, attractivité pour ses personnels (les conditions de travail sont un facteur évident d'attractivité pour ces professions) et coût raisonnable. J'ai eu l'occasion de visiter récemment tant les locaux de l'ANSSI que ceux du ComCyber à Rennes et je peux vous dire que nous sommes loin des conditions confortables de travail que peuvent offrir certaines grandes entreprises. Or, il ne faut pas se leurrer, c'est devenu aussi un élément d'attractivité et de fidélisation. Quand j'entends que des parlementaires ont critiqué la présence d'un babyfoot dans les locaux, je trouve la remarque déplacée et sans beaucoup d'égards pour des personnels rivés sur leurs écrans qui font un travail remarquable requérant une grande attention et générant beaucoup de stress et qui ont besoin de temps à autres d'un peu de détente.

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 ».

Nous devons toutefois vous informer que la Commission des finances a estimé nécessaire, dans un souci d'exemplarité, de réduire les crédits du Premier ministre. Elle a donc adopté un amendement pour réduire de 13,1 millions d'euros les crédits du programme « Coordination du travail gouvernemental », dont 1,5 million pour le titre 2 en les fléchant vers l'ANSSI.

Nous considérons que nos collègues ne font pas une juste analyse et donnent un mauvais signal. Nous avons mis en avant l'importance et la croissance des menaces, nous avons donné à l'ANSSI de nouveaux moyens, ce n'est pas en rabotant ses moyens que l'on réduira de façon significative les déficits publics, - on risque même de les accroître si demain il faut réparer les dommages qu'aura permis leur déficience. Cet amendement ne contribue pas à renforcer la sécurité nationale. Nous vous proposons donc si vous en êtes d'accord d'exprimer notre désaccord qui sera soumis au Sénat en séance publique lors de l'examen des crédits.

M. Jean-Marie Bockel. - Je voudrais rappeler la contribution de notre commission, dont un rapport d'information a amorcé la remontée en puissance de l'ANSSI dans le Livre blanc sur la défense et la sécurité nationale de 2013, puis dans la LPM 2014-2019, ce qui a permis de combler en partie le retard que nous avions avec les Américains, les Britanniques et les Allemands. Ce rapport a également conforté le volet militaire. Ceci montre l'importance des travaux parlementaires en ce domaine et la vigilance permanente que nous devons exercer sur les enjeux et les évolutions.

L'ANSSI est toujours confrontée à la sempiternelle question du turn over, il est aussi à la mesure de son succès. Au fur et à mesure que les entreprises et les administrations prennent conscience des risques et des enjeux, elles attirent à elles des ingénieurs passés par l'ANSSI. Cela devient une référence et, d'ailleurs, un élément d'attractivité pour les jeunes ingénieurs qui, jusqu'à présent, acceptaient une rémunération moins élevée que dans le privé avec la perspective d'une valorisation à l'issue. L'essaimage était un système gagnant-gagnant. Mais évidemment cela ne résout pas la tension liée à l'insuffisance des filières de formation en école d'ingénieur.

Je déplore, comme les rapporteurs, les retards de protection des administrations. Je vais être un peu cynique, mais souvent, tant qu'ils n'ont pas subi une attaque, il y a de la passivité. On ne devrait pas attendre un incident, mais c'est souvent celui-ci qui déclenche la prise de conscience au niveau décisionnaire. Hélas !

S'agissant de la coopération européenne, l'Union européenne doit agir dans le domaine des normes et sur le volet industriel, mais au-delà, quand on aborde les domaines de souveraineté, il faut bien discerner ce que l'on partage et avec qui. Le travail en bilatéral ou en trilatéral est souvent plus recommandé.

Enfin, je constate que, dans la presse, revient la question des produits chinois et des risques d'espionnage. Ceci est en partie le résultat des tensions commerciales actuelles. Là encore, il faut faire preuve de discernement dans les choix à opérer et bien distinguer les produits à risque en fonction des enjeux.

Mme Isabelle Raimond-Pavero. - Il est nécessaire de développer les moyens de l'ANSSI afin qu'elle donne aux entreprises et aux OIV les moyens de se défendre afin qu'ils ne fassent pas leur marché chacun de leur côté, ce qui représenterait un véritable danger.

Je suis inquiète car je pensais qu'il y avait un renforcement des crédits et j'entends parler de baisse. Il faut renforcer les moyens. Qu'est-ce qui est envisagé en dehors des recrutements qui exigent des formations longues? Peut-on agir efficacement au niveau européen ?

Enfin, il est important d'agir sur les comportements donc dans le domaine de l'éducation si on veut accroître la prise de conscience dans les entreprises et les administrations. Cela suppose d'agir sur les modes de penser, de concevoir et d'agir afin d'aboutir à un meilleur niveau de protection.

M. Richard Yung. - Nous sommes organisés en deux branches, l'une civile avec l'ANSSI et l'autre militaire. C'est un défaut français. Cela conduit sans doute à dupliquer beaucoup de choses. Peut-on tirer des éléments de réflexion des expériences étrangères ? Sans doute, encore que le modèle américain qui multiplie les agences ne soit pas le plus

vertueux. Supprimer les doublons pourrait dégager les moyens financiers dont nous avons besoin.

Mme Joëlle Garriaud-Maylam. - Sur le recrutement, je rappelle l'existence de la réserve citoyenne de cyberdéfense qui recrute énormément de jeunes, sortant d'école d'ingénieur, et accueille des spécialistes de cybersécurité. Peut-être est-ce un élément de réponse à ne pas négliger.

Pour votre information, je rentre du Forum de Dakar avec nos collègues Perrin et Cazeau où le ministre de l'Europe et des affaires étrangères a annoncé la création dans cette ville d'une école de cybersécurité qui aura pour vocation de former des spécialistes originaires de toute la région.

Enfin, nous devrions nous poser la question de la souveraineté numérique au niveau européen. J'avais déposé une proposition de résolution pour créer une commission d'enquête sur nos liens Microsoft qui sont un élément de vulnérabilité considérable au niveau européen et français. Il y a eu de nombreux problèmes d'attaques à travers ces logiciels et nos gouvernements et nos administrations continuent à les utiliser, alors que nous prônons une autonomie stratégique européenne. A contrario, il faut s'en féliciter, la gendarmerie travaille avec des logiciels libres et ses applications sont moins vulnérables.

M. Rachel Mazuir. - Jean-Marie Bockel et notre collègue Jacques Berthou avaient réalisé un travail remarquable en 2012.

La préservation de notre souveraineté est un enjeu majeur surtout dans le contexte européen actuel, mais il est important qu'il y ait une information fluide entre les Etats sur les cyberattaques dès leur détection. Le cyberespace n'a guère de frontière ; en anticipant la détection, on peut mieux se prémunir.

S'agissant de la formation des ingénieurs et m'appuyant sur des exemples étrangers, peut-être faut-il être plus incitatif, par un système de bourses par exemple.

Sur l'organisation de la cybersécurité, le périmètre du Commandement Cyber est très circonscrit, c'est celui du ministère des armées (hors services de renseignement). En revanche, celui de l'ANSSI est très large puisqu'elle intervient vis-à-vis des administrations de l'Etat, mais aussi des opérateurs d'importance vitale, 219 entités dans les secteurs les plus divers et doit mener une politique de sensibilisation et d'appui pour toute la société : entreprises, collectivités....La cybersécurité nous concerne tous dès lors que nous sommes connectés, nous devenons vulnérables et potentiellement victimes de cybercriminels.

M. Olivier Cadic. - Le Sénat a, en effet, joué un rôle de lanceur d'alerte dans le domaine de la cybersécurité comme Jean-Marie Bockel l'a souligné.

Je voudrais préciser, en réponse à Isabelle Raimond-Pavero, que les crédits de l'ANSSi progressent dans le projet de loi de finances pour 2019, simplement la commission des finances va déposer un amendement pour les réduire. Nous estimons que ce n'est pas une bonne idée. L'effort de l'ANSSI doit être soutenu. C'est une priorité. Donc, je partage son inquiétude.

Vis-à-vis des entreprises, il faut distinguer les opérateurs d'importance vitale (OIV) sur lesquels pèsent des obligations réglementaires d'assurer leur cybersécurité, des autres entreprises pour lesquelles l'ANSSI n'intervient que pour sensibiliser et favoriser l'émergence de produits et de services dont elle soutient le développement, qu'elle référence et labellise.

Pour répondre à Richard Yung, l'organisation française préserve l'autonomie des armées, notamment sur le volet opérationnel de leur cybersécurité, dont la confidentialité doit être préservée et qui relève du Commandement Cyber et les autres secteurs de l'Etat qui relèvent de l'ANSSI. Cette répartition présente aussi un grand avantage par rapport à l'organisation adoptée dans d'autres pays dans lesquels la cybersécurité relève des agences

techniques de renseignement, notamment en ce qu'elle ne provoque aucune ambiguïté quant aux interventions de l'ANSSI et les rend plus faciles. Lorsque je rencontre des interlocuteurs dans ce domaine et que nous abordons ces sujets, j'ai tendance à leur dire que si cette organisation leur convient, s'ils y sont confortables et si elle leur permet d'agir avec efficacité, c'est qu'elle est pertinente. Pour autant, il ne faut pas en faire un totem et il faudra savoir la faire évoluer si elle perd en efficacité.

S'agissant de la réserve de cyberdéfense, j'étais récemment à Rennes au Commandement Cyber et me suis entretenu avec les responsables en charge des réserves. Effectivement, comme l'a rappelé Joëlle Garriaud-Maylam, il y a un nombre important de réservistes citoyens. C'est encourageant, mais il faut déterminer les missions susceptibles de leur être confiées et réaliser l'adéquation entre les missions, les profils et leur disponibilité. Un travail de réflexion et d'organisation est en cours.

S'agissant de la gendarmerie et de la police, elles prennent résolument le virage de la numérisation avec le déploiement de terminaux sécurisés dans le cadre du dispositif NéO avec le concours de l'ANSSI.

Dans le domaine capacitaire européen, un partenariat public-privé dédié à la cybersécurité a été lancé par la Commission avec pour objectif de générer 1,8 milliard d'euros d'investissements via l'effet de levier de 450 millions de 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.

Enfin, il a été cité une marque de logiciel grand public américaine, ce n'est sans doute pas la menace principale. Il y a d'autres logiciels vecteurs porteurs de vulnérabilité, y compris certains anti-virus... mais le maillon de vulnérabilité, c'est souvent l'utilisateur avant l'outil, c'est nous quand nous ne mettons pas à jour nos logiciels, quand nous n'installons pas de VPN (virtual private network) sur nos portables lorsque nous nous rendons à l'étranger... Enfin, il ne faut pas méconnaître la diversité des menaces en ce qui concerne notre indépendance et notre autonomie dans ce domaine, notamment dans la compétition économique. N'oublions pas que les entreprises françaises peuvent se développer aux États-Unis, c'est rarement le cas en Chine. Enfin, nous aurons l'occasion d'entendre M. Sarts, responsable du centre d'excellence de l'OTAN, le 19 décembre qui pourra nous présenter un panorama des menaces du point de vue de cette organisation.

M. Jean-Marie Bockel. - Simplement, pour compléter les propos des rapporteurs sur l'organisation française, elle est plus récente donc a su éviter les pièges des modèles antérieurs. Elle est excellente d'un double point de vue. D'un point de vue militaire, elle comprend les volets défensif et offensif qui vont de pair et donnent une capacité complète à nos armées. D'un point de vue fonctionnel, elle ne suscite pas de rivalités, bien au contraire. Il est significatif que les lois de programmation militaire servent de véhicules pour les avancées législatives renforçant les compétences et les moyens d'action de l'ANSSI.

M. Christian Cambon, président. - Nous allons procéder au vote sur les crédits de la mission qui font l'objet d'un avis favorable des rapporteurs.

La commission donne un avis favorable à l'adoption des crédits de la mission «Direction de l'action du Gouvernement », les sénateurs du groupe CRCE s'abstenant.

ANNEXE – LISTE DES AUDITIONNÉS

➢ **Audition en commission plénière :**

- Mercredi 3 octobre 2018 :

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

Compte-rendu consultable sur le site Internet du Sénat à l'adresse suivante :
http://www.senat.fr/compte-rendu-commissions/20181001/etr.html#toc8

➢ **Déplacement :**

- Jeudi 18 octobre 2018

Visite de l'agence nationale de la sécurité des systèmes d'information (ANSSI)