

N° 142

# SÉNAT

SESSION ORDINAIRE DE 2019-2020

---

---

Enregistré à la Présidence du Sénat le 21 novembre 2019

## 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 2020,*

TOME IX

**DIRECTION DE L'ACTION DU GOUVERNEMENT :**  
Coordination du travail gouvernemental (Programme 129)

Par MM. Olivier CADIC et Rachel MAZUIR,

Sénateurs

---

(1) Cette commission est composée de : M. Christian Cambon, *président* ; MM. Pascal Allizard, Bernard Cazeau, Olivier Cigolotti, Robert del Picchia, Jean-Noël Guérini, Joël Guerriau, Pierre Laurent, Cédric Perrin, Gilbert Roger, Jean-Marc Todeschini, *vice-présidents* ; Mme Joëlle Garriaud-Maylam, M. Philippe Paul, Mme Marie-Françoise Perol-Dumont, M. Olivier Cadic, *secrétaires* ; MM. Jean-Marie Bockel, Gilbert Bouchet, Michel Boutant, Alain Cazabonne, Pierre Charon, Mme Hélène Conway-Mouret, MM. Édouard Courtial, René Danesi, Gilbert-Luc Devinaz, Jean-Paul Émorine, Bernard Fournier, Mme Sylvie Goy-Chavent, MM. Jean-Pierre Grand, Claude Haut, Mme Gisèle Jourda, MM. Jean-Louis Lagourgue, Robert Laufoaulu, Ronan Le Gleut, Jacques Le Nay, Rachel Mazuir, François Patriat, Gérard Poadja, Ladislav 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<sup>ème</sup> législ.) : 2272, 2291, 2292, 2298, 2301 à 2306, 2365, 2368 et T.A. 348

Sénat : 139 et 140 à 146 (2019-2020)



## SOMMAIRE

Pages

<b>PRINCIPALES OBSERVATIONS</b> .....	7
<b>INTRODUCTION</b> .....	9
<b>TITRE PREMIER : LE SECRETARIAT GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE (SGDSN) ET LES ENTITÉS RELEVANT DU PROGRAMME 129</b> .....	11
<b>I. LE SGDSN, OUTIL INTERMINISTÉRIEL DE PRÉVENTION ET DE GESTION DES CRISES : L'EXEMPLE DU CONTRÔLE DES EXPORTATIONS DE MATÉRIELS DE GUERRE</b> .....	11
A. COMPOSITION DE LA CIEEMG ET PROCÉDURE D'EXAMEN DES DEMANDES...	11
B. ACTIVITÉS DE LA CIEEMG.....	12
C. INFORMATION DU PARLEMENT .....	13
<b>II. LE SGDSN, ACTEUR DE LA POLITIQUE DE SÉCURITÉ NATIONALE</b> .....	13
A. LE RENFORCEMENT DES POLITIQUES DE PROTECTION CONTRE LES MENACES ET RISQUES MAJEURS .....	13
1. <i>Le renforcement de la sécurité dans les transports</i> .....	13
2. <i>La mise en œuvre de plan d'action contre le terrorisme (PACT)</i> .....	14
3. <i>L'action en matière de résilience et le renforcement de la continuité des activités essentielles à la Nation</i> .....	14
B. LA RÉFORME DE LA RÉGLEMENTATION RELATIVE À LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE .....	14
<b>III. L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI), BRAS ARMÉ DE L'ÉTAT POUR LA CYBERDÉFENSE</b> .....	16
A. UNE MENACE QUI NE CESSE DE S'ACCROÎTRE EN INTENSITÉ ET EN SOPHISTICATION .....	16
B. LA LENTE MISE EN ŒUVRE DE LA POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT (PSSIE) .....	16
1. <i>Les services de l'État, cibles de nombreuses cyberattaques</i> .....	17
2. <i>Un inquiétant état de vulnérabilité des services de l'État</i> .....	18
3. <i>L'engagement d'un travail interministériel de remédiation</i> .....	19
4. <i>Une nouvelle feuille de route</i> .....	20
5. <i>Le nécessaire renforcement des moyens juridiques de l'ANSSI pour le contrôle des grands projets de l'Etat</i> .....	20
C. L'ÉLARGISSEMENT DU PÉRIMÈTRE D'ACTION .....	22
1. <i>La transposition de la « directive NIS »</i> .....	22
2. <i>La protection des réseaux</i> .....	23

---

D. L'ANSSI, ACTEUR DE LA CONSOLIDATION DE LA FILIÈRE FRANÇAISE DE SÉCURITÉ INFORMATIQUE .....	24
<b>IV. LE GROUPEMENT INTERMINISTÉRIEL DE CONTRÔLE (GIC).....</b>	<b>25</b>
A. L'ACCROISSEMENT DE SON ACTIVITÉ .....	25
B. LES ENJEUX À MOYEN TERME.....	26
<b>TITRE 2 : LES MOYENS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2020 .....</b>	<b>27</b>
<b>I. LES CRÉDITS DE TITRE 2 ET LA POLITIQUE DES RESSOURCES HUMAINES...29</b>	
A. LES CRÉDITS ET LES EMPLOIS INSCRITS AU BOP SGDSN .....	29
B. LE SGDSN : UNE VIGILANCE À GARDER SUR L'ORGANISATION DES FONCTIONS DE SOUTIEN .....	29
C. L'ANSSI : UNE NÉCESSAIRE REMONTÉE EN PUISSANCE DES EFFECTIFS .....	30
D. LE GIC : GARDER LA MAÎTRISE DES EFFECTIFS ET ASSURER LEUR MONTÉE EN PUISSANCE.....	31
<b>II. LES CRÉDITS DE FONCTIONNEMENT ET D'INVESTISSEMENT INSCRITS AU « BOP » SGDSN .....</b>	<b>32</b>
A. SGDSN/ANSSI : DES ACTIONS NOMBREUSES ET DIVERSES À SOUTENIR (LES CRÉDITS HORS TITRE 2 EN PLF 2019) .....	32
1. L'ANSSI représente une part importante des crédits hors titre 2 .....	33
2. Crédits de fonctionnement de l'ensemble SGDSN/ANSSI (hors GIC et subvention aux opérateurs) .....	33
3. Les dépenses d'investissement .....	34
4. Les dépenses d'intervention .....	35
B. LE MAINTIEN DE L'EFFORT BUDGÉTAIRE POUR ACCOMPAGNER L'ACTIVITÉ DU GIC .....	35
1. Les crédits de fonctionnement .....	35
2. Les crédits d'investissement .....	36
<b>III. LES FONDS SPÉCIAUX : DES CRÉDITS EN CROISSANCE .....</b>	<b>37</b>
<b>TITRE 3 : LES INSTITUTS RATTACHÉS AU SGDSN .....</b>	<b>39</b>
<b>I. L'INSTITUT DES HAUTES ÉTUDES DE DÉFENSE NATIONALE .....</b>	<b>40</b>
A. MISSIONS ET ACTIVITÉS DE L'IHEDN.....	40
1. Un plan stratégique 2020-2022 qui n'est toujours pas adossé à un contrat d'objectifs et de performances.....	40
2. Les activités de l'IHEDN .....	41
B. L'ÉVOLUTION DES CRÉDITS ET DES EMPLOIS DE L'IHEDN .....	42
<b>II. L'INSTITUT NATIONAL DES HAUTES ÉTUDES DE LA SÉCURITÉ ET DE LA JUSTICE.....</b>	<b>43</b>

A. MISSIONS ET ACTIVITÉS DE L'INHESJ .....	44
1. <i>Les missions formalisées dans un plan stratégique.....</i>	44
2. <i>Le contrat d'objectifs et de performances : un outil de pilotage.....</i>	44
3. <i>Les activités de formation et de recherche .....</i>	44
B. L'ÉVOLUTION DES CRÉDITS ET DES EMPLOIS DE L'INHESJ .....	45
1. <i>Un développement financé par des ressources propres .....</i>	45
2. <i>Des effectifs plafonnés et maîtrise de la progression de la masse salariale .....</i>	45
<b>III. LE RAPPROCHEMENT ENGAGÉ ENTRE L'IHEDN ET L'INHESJ .....</b>	<b>46</b>
<b>EXAMEN EN COMMISSION.....</b>	<b>47</b>
<b>LISTE DES PERSONNES AUDITIONNÉES .....</b>	<b>49</b>



## PRINCIPALES OBSERVATIONS

**L'avis de la commission porte sur les crédits du SGDSN, de l'ANSSI, du GIC, de l'IHEDN, de l'INHESJ et sur les fonds spéciaux figurant à l'action 2 du programme 129.**

**Le Titre 2 connaît une évolution paradoxale.** Les crédits sont en baisse de 17,8 % alors que les schémas d'emploi font apparaître une création nette de 55 emplois au profit de l'ANSSI et du GIC et que des mesures de desserrement salarial ont été décidées pour recruter et fidéliser dans les métiers sous tension. Cette évolution résulte de la prise en charge des rémunérations des militaires affectés au SGDSN et dans les entités qui en dépendent par les crédits du ministère des Armées. Cet arrangement n'est pas conforme à l'esprit de la LOLF et va compliquer l'exercice du contrôle parlementaire et son appréciation du coût complet de fonctionnement du SGDSN et des entités qui en dépendent.

**Recommandation n° 1 :** Réintégrer ces rémunérations dans le programme 129. A défaut, créer un article spécifique dans le programme 212 de la mission « Défense »

**Les effectifs de l'ANSSI reprennent une progression en adéquation avec l'élargissement de ses missions.** La commission avait, à plusieurs reprises, attiré l'attention du Gouvernement sur le risque que constituait le ralentissement de leur montée en puissance. Elle se réjouit de cette décision.

**L'intensification de la menace exige une rénovation de la politique de sécurité des systèmes d'information de l'Etat.** La commission a attiré depuis plusieurs années l'attention du Gouvernement sur la vulnérabilité croissante des administrations et de leurs opérateurs à raison de la numérisation croissante de leurs activités. Le Premier ministre a engagé une politique de rénovation de la politique de sécurité des systèmes d'information de l'Etat (PSSIE), une feuille de route va être mise en œuvre par l'ANSSI. Le décret créant la DInum renforce la capacité de supervision de l'ANSSI. La commission soutient cet effort. Elle souhaite néanmoins que cette supervision interministérielle soit renforcée et durcie.

**Recommandation n° 2 :** Renforcer la supervision par l'ANSSI dans le décret du 25 octobre 2019.

**Recommandation n° 3 :** Mettre en place des dispositifs d'incitation/sanction sur le financement des projets en fonction de la prise en compte des normes de sécurité.

**Recommandation n° 4 :** Imposer aux DNum ministériels et aux directeurs « métiers » pilotant la mise en œuvre de projets numériques une formation solide évaluée par l'ANSSI, inscrire des objectifs en matière de sécurité informatique définis par l'ANSSI dans leurs lettres de mission et prendre en compte ces objectifs dans leur évaluation.

**La commission regrette la suppression de l'INHESJ** qu'elle estime incompréhensible au regard des missions et des objectifs de cet établissement. Elle craint que cette décision n'affaiblisse la nécessaire coordination et le travail commun réalisé dans le domaine de la recherche et de la formation par l'intérieur et la justice et doute de son bienfondé économique.

**Elle se réjouit de la poursuite de l'activité de l'IHEDN et de la qualité de son plan stratégique 2019-2022 mais s'inquiète de sa soutenabilité économique sans moyens supplémentaires, d'autant que l'IHEDN devra absorber seul à compter de 2021 les charges mutualisées avec l'INHESJ et reprendre certaines des formations dispensées dans le domaine de la sécurité nationale.**



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 la 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	712,9	692,6	2965
ACTION 2	387,8	354,3	1267
RATIO ACTION2/P129	54,40%	51,15%	41,37%

Sources : PLF 2020

L'action 2 est dotée dans le projet de loi de finances pour 2020 de **387,13 M€** en autorisations d'engagement (AE) et **354,32 M€** de crédits de paiement (CP). Ces crédits progressent de **2,85% en AE** et diminuent de **1,77% en CP**.

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

	LFI 2019		PLF 2020	
	AE	CP	AE	CP
<b>SGDSN</b>	<b>279 463 893</b>	<b>263 087 897</b>	<b>282 654 698</b>	<b>249 150 197</b>
Titre2	83 387 271	83 387 271	68 689 571	68 689 571
Hors titre 2	196 076 622	179 700 626	213 965 127	180 460 626
<b>Fonds spéciaux</b>	<b>66 804 810</b>	<b>66 804 810</b>	<b>76 804 810</b>	<b>76 804 810</b>
<b>GIC</b>	<b>30 789 887</b>	<b>30 801 704</b>	<b>28 354 081</b>	<b>28 365 898</b>
Titre2	13 819 526	13 819 526	11 383 720	11 383 720
Hors titre 2	16 970 361	16 982 178	16 970 361	16 982 178
<b>Total action 2</b>	<b>377 058 590</b>	<b>360 694 411</b>	<b>387 813 589</b>	<b>354 320 905</b>

Sources : Réponse au questionnaire parlementaire

Cette action expose **les moyens du Secrétariat général de la défense et de la sécurité nationale (SGDSN) et 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 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 subvention pour charge de service public.



## TITRE PREMIER : LE SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE (SGDSN) ET LES ENTITES RELEVANT DU PROGRAMME 129

Dans ses précédents avis<sup>1</sup>, la commission a exposé en détail les activités du SGDSN et des entités relevant du programme 129. Le présent avis ne retrace que les évolutions significatives intervenues en 2019 et les perspectives 2020 sans souci d'exhaustivité.

### I. LE SGDSN, OUTIL INTERMINISTÉRIEL DE PRÉVENTION ET DE GESTION DES CRISES : L'EXEMPLE DU CONTRÔLE DES EXPORTATIONS DE MATÉRIELS DE GUERRE

Le SGDSN est l'outil du Gouvernement pour le traitement des sujets sensibles en matière de défense et de sécurité nationale

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)<sup>2</sup>. Il participe, en outre, aux travaux internationaux sur les biens à double usage et apporte son expertise à la commission interministérielle des biens à double usage (CIBDU) pour l'instruction des dossiers sensibles.

#### A. COMPOSITION DE LA CIEEMG ET PROCÉDURE D'EXAMEN DES DEMANDES

Lors de son audition par la commission, le 2 octobre<sup>3</sup>, Mme Claire Landais, secrétaire générale de la défense et de la sécurité nationale a indiqué que « *Les avis de la commission sont rendus dans un esprit de consensus ; si tel n'est pas le cas, le dossier est soumis à la délibération du cabinet du Premier ministre. Les jeux d'acteurs ne sont pas figés : ce n'est pas toujours le ministère de l'économie qui veut vendre, le ministère des affaires étrangères qui évoque le respect des engagements internationaux, et le ministère des armées qui ne tiendrait compte que de ses partenariats stratégiques ! Au contraire, une véritable discussion s'instaure.*

*L'arbitrage fonctionne avec un verrou d'entrée, qui est le respect de nos engagements internationaux, dont les deux principaux sont la position commune de 2008 de l'Union européenne et le traité sur le commerce des armes signé en 2014.*

---

<sup>1</sup> [Sé debates n° 149 Tome IX \(2018-2019\) par MM. Cadic et Mazuir](#)

<sup>2</sup> Loi n° 2011-702 du 22 juin 2011.

<sup>3</sup> <http://www.senat.fr/compte-rendu-commissions/20190930/etr.html#toc3>

*Nous devons nous baser sur nos connaissances, lesquelles sont constituées de sources publiques - les documents produits par les experts de l'ONU, par exemple - et de nos sources propres, notamment fournies par nos services de renseignement, pour déterminer si l'équipement qui fait l'objet de la demande de licence est susceptible de conduire à un risque « prépondérant », pour reprendre les termes du traité sur le commerce des armes, ou « manifeste », pour reprendre ceux de la position commune, d'utilisation qui serait contraire à un certain nombre de principes du droit international, notamment en matière de droits de l'homme.*

*Les grands principes à respecter sont la discrimination entre les populations civiles et les combattants, la discrimination entre les objets civils et les objectifs militaires, l'interdiction de dommages collatéraux disproportionnés par rapport à l'avantage militaire attendu d'une attaque et le principe d'humanité, selon lequel il faut chercher à limiter les dommages collatéraux d'une attaque.*

*Si l'on considère que la demande de licence respecte nos engagements internationaux, d'autres considérations sont alors prises en compte : la sécurité de nos forces et de celles de nos alliés, la préservation de notre base industrielle et technologique de défense, et des considérations économiques. En effet, certains programmes dont nous avons besoin au niveau national ne sont économiquement rentables que si nous les exportons ».*

#### **Composition et procédure d'examen des demandes**

La CIEEMG est composée de quatre membres à voix délibérative, qui doivent être consultés pour l'établissement des avis sur les opérations d'exportation ou de transfert. Ces membres à voix délibérative représentent respectivement la secrétaire générale de la défense et de la sécurité nationale, le ministre de l'Europe et des affaires étrangères, le ministre des armées et le ministre de l'économie et des finances.

Les avis de la CIEEMG sont rendus soit par voie dématérialisée, essentiellement au moyen du système d'information SIGALE, soit par voie écrite, au moyen des comptes rendus des séances plénières mensuelles de la CIEEMG.

Les dossiers les plus sensibles ou pour lesquels un avis défavorable est émis sont systématiquement examinés en réunion plénière. Tous les participants doivent être habilités au niveau « Secret défense ».

Les avis de la CIEEMG sont rendus sur la base du consensus entre les membres à voix délibérative. En cas de difficulté pour dégager ce consensus ou de besoin de concertation à haut niveau, la formulation de l'avis peut être repoussée à la consultation du cabinet du Premier ministre.

## **B. ACTIVITÉS DE LA CIEEMG**

Sur la période d'août 2018 à août 2019<sup>1</sup>, la CIEEMG s'est prononcée sur 7 027 dossiers (en hausse de 11%) correspondant à 5 090 dépôts de nouvelles « demandes de licence » (stable par rapport à l'année précédente) et 1 937 demandes de « modification de licences » déjà accordées (soit 27%

<sup>1</sup> On trouvera dans [l'avis budgétaire sur le PLF 2019](#), les éléments pour la période août 2017-août 2018.

environ). Environ 95% des demandes ont fait l'objet d'un traitement en procédure « continue »<sup>1</sup> avec avis favorable. 62% 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 486 dossiers, soit un peu moins que sur la précédente période de douze mois, pour lesquels elle a prononcé 359 avis favorables et 127 avis défavorables soit 26% des dossiers<sup>2</sup>.

### **C. INFORMATION DU PARLEMENT**

Le ministère des armées transmet chaque année au parlement un rapport sur les exportations d'armements<sup>3</sup>.

**Le Président Christian Cambon a indiqué que « l'Assemblée nationale et le Sénat réfléchissent actuellement à des nouveaux moyens d'accroître le contrôle du parlementaire, dans le respect des compétences du Gouvernement ».**

## **II. LE SGDSN, ACTEUR DE LA POLITIQUE DE SÉCURITÉ NATIONALE**

### **A. LE RENFORCEMENT DES POLITIQUES DE PROTECTION CONTRE LES MENACES ET RISQUES MAJEURS**

#### **1. Le renforcement de la sécurité dans les transports**

Dans le cadre du renforcement de la sécurité aérienne et aéroportuaire, il a poursuivi ses travaux pour lutter contre l'usage malveillant des drones civils afin de fixer le cadre d'emploi des systèmes de brouillage<sup>4</sup>.

Conformément aux annonces réalisées lors du sommet de Sandhurst en janvier 2018, le SGDSN, en collaboration avec les ministères concernés et les autorités britanniques, a élaboré un projet d'accord intergouvernemental (AIG) consacré à la sûreté maritime et portuaire en Manche et en mer du Nord. Ce projet a été présenté aux autorités britanniques le 1<sup>er</sup> juillet 2019.

---

<sup>1</sup> Demandes traitées de manière dématérialisée dans le système d'information SIGALE.

<sup>2</sup> Les dossiers les plus sensibles ou pour lesquels un avis défavorable est émis sont systématiquement examinés en réunion plénière.

<sup>3</sup> <https://www.defense.gouv.fr/content/download/559159/9678968/RAP%202019-Parties%201-2-3%2BAnnexes.pdf>

<sup>4</sup> Ainsi, dans le cadre des appels à manifestation d'intérêt (AMI) pour les Jeux olympiques de Paris 2024, un bilan des capacités de neutralisation de drones dans un contexte de grands événements sera réalisé à l'occasion d'une démonstration qui se tiendra à Avignon les 16 et 17 octobre 2019.

## **2. La mise en œuvre de plan d'action contre le terrorisme (PACT)**

Le SGDSN assure le suivi de la mise en œuvre du PACT<sup>1</sup>, en liaison avec la CNRLT. Fin juin 2019, 15 actions du PACT sur 32 sont réalisées, et 17 sont en cours de réalisation.

## **3. L'action en matière de résilience et le renforcement de la continuité des activités essentielles à la Nation**

Le SGDSN a mis en place un dialogue national de sécurité dont l'objectif est de promouvoir les échanges entre les pouvoirs publics et les représentants de secteurs professionnels jugés sensibles<sup>2</sup>. Après les opérateurs des centres commerciaux en 2017, les représentants des festivals et des grands événements en mai 2018, ceux des parcs de loisir (octobre 2018), la question des établissements patrimoniaux a été abordée (juin 2019).

Enfin, le SGDSN a réalisé une plateforme « en ligne » de sensibilisation à la menace terroriste, de formation au plan Vigipirate et aux réactions à adopter en cas d'attaque, destinée au grand public, aux exploitants d'établissements recevant du public et aux élus locaux<sup>3</sup>.

## **B. LA RÉFORME DE LA RÉGLEMENTATION RELATIVE À LA PROTECTION DU SECRET DE LA DÉFENSE NATIONALE**

Les articles 413-9 et suivants du code pénal définissent le secret de la défense nationale et le régime répressif de la compromission. Dans le code de la défense se trouve la partie « haute » de la réglementation et un renvoi à une instruction générale interministérielle IGI n° 1300 du 30 novembre 2011. Une importante concertation interministérielle a été 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.

Le calendrier prévisionnel permet d'envisager une publication du projet de décret à l'automne 2019, une finalisation des travaux rédactionnels de la nouvelle instruction générale n° 1300 d'ici la fin de l'année, et une entrée en vigueur de la réforme au 1<sup>er</sup> janvier 2021. Cette réforme a été engagée depuis plusieurs années, il serait souhaitable que le calendrier soit respecté.

Caractérisée par le passage de trois niveaux (Confidentiel Défense, Secret Défense, Très Secret Défense) à deux niveaux de classification (Très secret, Secret), la réforme vise à :

---

<sup>1</sup> Voir également [Sénat n° 149 Tome IX \(2018-2019\)](#) par MM. Cadic et Mazuir p. 16.

<sup>2</sup> En dehors des opérateurs d'importance vitale (OIV) pour lesquels un cadre d'échange existe déjà.

<sup>3</sup> <https://vigipirate.gouv.fr/>

- inciter à moins et mieux classifier grâce à la simplification des niveaux de classification ;
- aligner les mesures de protection associées à chaque niveau de classification sur les standards internationaux afin de mieux protéger les informations échangées avec nos partenaires étrangers, sans nuire aux exigences opérationnelles ;
- mieux prendre en compte la dimension « sécurité des systèmes d'informations » dans la protection des informations classifiées.

La réforme est conçue de façon à limiter au mieux l'impact organisationnel pour les structures qui émettent, manipulent ou détiennent des informations classifiées<sup>1</sup>.

S'agissant de la formation à la protection du secret, chaque personne habilitée fait l'objet d'une sensibilisation par l'officier de sécurité dont elle relève. Cette sensibilisation offre l'occasion de rappeler les obligations des personnes habilitées au regard du code pénal et de préciser les règles relatives à la gestion matérielle et dématérialisée des informations et supports classifiés. Elle permet également de présenter les techniques d'approche des groupes subversifs et des organisations étrangères, en particulier sur le territoire national. Cela peut être complété par des séances de sensibilisation communes, internes à l'organisme, des entretiens individualisés ou encore la distribution de plaquettes d'information et de guides pratiques.

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.

**La commission avait souhaité que l'effort de formation continue engagé en direction des administrations et des entreprises des secteurs sensibles<sup>2</sup> soit prolongé par une formation initiale 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. Ils regrettent qu'aucune avancée n'ait été réalisée en 2019 en ce domaine.**

**Elle se réjouit de l'initiative de sensibilisation des parlementaires à la problématique de protection des données sensibles et notamment des conseils apportés concernant leurs déplacements à l'étranger.**

---

<sup>1</sup> Ainsi, les documents classifiés produits avant l'entrée en vigueur de la réforme ne seront pas remarqués ; les annexes de sécurité, les avis de sécurité et les décisions d'homologation en cours de validité resteront en vigueur jusqu'à la date normale de leur renouvellement. Aucune nouvelle norme de protection physique ni bâtiminaire ne sera mise en place.

<sup>2</sup> [Voir également Sénat n° 149 Tome IX \(2018-2019\) par MM. Cadic et Mazuir p. 17.](#)

### 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<sup>1</sup>, le SGDSN dispose de l'ANSSI<sup>2</sup>. 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 projet annuel de performances (voir infra p. 28).

La *Revue stratégique de cyberdéfense*<sup>3</sup> 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 élargi ses missions<sup>4</sup> comme celui mis en place par la **loi n° 2019-810 du 1<sup>er</sup> août 2019 visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles**<sup>5</sup>.

#### 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<sup>6</sup>. Dans son rapport d'activité<sup>7</sup>, 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 ».

#### B. LA LENTE MISE EN ŒUVRE DE LA POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION DE L'ÉTAT (PSSIE)

La Politique de sécurité des systèmes d'information de l'État (PSSIE) établit un socle de mesures techniques et organisationnelles visant à assurer la protection des systèmes d'information de l'administration face à des

---

<sup>1</sup> Article R 312-3 du code de la défense.

<sup>2</sup> Service à compétence nationale (décret n° 2009-834 du 7 juillet 2009 modifié).

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

<sup>4</sup> L'article 34 de la loi n° 2018-607, relative à la programmation militaire pour les années 2019-2025, lui confère de nouvelles prérogatives en matière de détection, de caractérisation et de prévention des attaques informatiques en collaboration étroite avec les opérateurs de communications électroniques et les hébergeurs.

<sup>5</sup> <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000038864094&categorieLien=id>

<sup>6</sup> <http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf>

<sup>7</sup> [https://www.ssi.gouv.fr/uploads/2019/04/anssi\\_rapport\\_annuel\\_2018.pdf](https://www.ssi.gouv.fr/uploads/2019/04/anssi_rapport_annuel_2018.pdf)



cyberattaques de niveau faible à modéré. **Le Premier ministre a publié, en 2014, une circulaire fixant** les contours d'une « *Politique de sécurité des systèmes d'information de l'État* » (PSSIE)<sup>1</sup> **et des règles de protection**<sup>2</sup>. Elle constitue un élément de réponse essentiel aux cybermenaces.

**Dans ses avis sur les PLF 2017<sup>3</sup>, 2018<sup>4</sup> et 2019<sup>5</sup>, la commission s'inquiétait de la lenteur de ce processus. Les résultats ne se sont guère améliorés. La RCS<sup>6</sup> de février 2018 avait confirmé cette situation consternante et alarmante.**

## **1. Les services de l'État, cibles de nombreuses cyberattaques**

Afin de mesurer concrètement la vulnérabilité des administrations de l'État aux cyberattaques, la Commission a demandé, dans le cadre du questionnaire parlementaire, la communication par ministère, du nombre d'incidents consécutifs à des cyberattaques ayant fait l'objet d'une intervention de l'ANSSI.

Entre le 1<sup>er</sup> janvier et le 31 décembre 2018, l'ANSSI a été amenée à traiter 78 événements de sécurité consécutifs à des attaques informatiques ayant touché des ministères français. Il est à noter que ces différents événements ont requis un niveau variable d'engagement et d'expertise des agents de l'ANSSI, en fonction de la nature et du niveau technique de l'attaque ainsi que du périmètre et de l'impact de la compromission.

Ainsi, sur ces 78 incidents, 31 se sont révélés mineurs au sens où un engagement minimal a été requis pour leur traitement, 32 peuvent être qualifiés de notables puisque demandant l'emploi d'expertises particulières pour leur résolution, alors que 15 se sont avérés majeurs nécessitant pour leur traitement un engagement et une expertise importants et de moyen à long-terme de la part de l'ANSSI (trois d'entre eux ont d'ailleurs fait l'objet d'une opération de cyberdéfense<sup>7</sup>).

---

<sup>1</sup> 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.

<sup>2</sup> n° 5725/SG du 17 juillet 2014.

<sup>3</sup> Sénat n° 142 Tome IX (2016-2017) par MM. Bockel et Masseret, p. 37 et suiv.

<sup>4</sup> 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>

<sup>5</sup> Sénat n° 149 Tome IX (2018-2019) par MM. Cadic et Mazuir p. 22 et suiv.

<sup>6</sup> <http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf>  
p. 56 et suiv.

<sup>7</sup> Une opération de cyberdéfense menée par l'ANSSI entend répondre à un incident de sécurité majeur menaçant directement les systèmes numériques et compromettant les opérations liées à l'activité d'une ou plusieurs organisations d'importance vitale ou fortement sensibles. Elle requiert la mobilisation, sur un temps long, de compétences transverses au sein de l'Agence.

Tableau du nombre d'incidents, par ministère, consécutifs à des attaques informatiques<sup>1</sup>

Ministères	Incidents traités par l'ANSSI	Commentaires
Ministère de l'agriculture et de l'alimentation	6	Dont un incident majeur
Ministère de la cohésion des territoires	1	
Ministère de la culture	4	
Ministère des armées	4	Dont deux incidents majeurs
Ministère de l'économie et des finances	9	Dont deux incidents majeurs
Ministère de l'éducation nationale et de la Jeunesse	24	Dont un incident majeur
Ministère de l'enseignement supérieur et de la recherche	2	
Ministère de l'Europe et des affaires étrangères	11	Dont trois opérations de cyberdéfense et quatre incidents majeurs
Ministère de l'intérieur	9	Dont deux incidents majeurs
Ministère de la justice	8	Dont trois incidents majeurs
Ministère des outre-Mer	1	
Ministère des solidarités et de la santé	8	Dont deux incidents majeurs
Ministère de la transition écologique et solidaire	3	
Ministère du travail	1	

Sources : Réponses au questionnaire parlementaire

Au sein du ministère des armées, le commandement de la cyberdéfense (COMCYBER), créé en 2017, assure la détection des attaques informatiques sur l'essentiel des systèmes ministériels. En 2018, le ministère a traité 19 incidents, dont 4 en collaboration avec l'ANSSI.

La surface d'exposition de certains ministères est grande (il s'agit de la somme des vulnérabilités d'un système d'information pouvant être exploitées par un attaquant informatique), de par le nombre d'entités sous leur tutelle ou le nombre de leurs emprises territoriales. Ceux-ci sont donc susceptibles d'être victimes d'un plus grand nombre d'attaques informatiques réussies.

## 2. Un inquiétant état de vulnérabilité des services de l'État

Si l'on constate une meilleure prise en compte des enjeux par les autorités, l'importance de la menace montre que les réponses restent, à ce jour, insuffisantes et maintiennent nos administrations dans un état de vulnérabilité inquiétant.

---

<sup>1</sup> Il est à noter qu'un même incident peut impacter plusieurs ministères dans le même temps. C'est pourquoi la somme des données du tableau est différente de celle fournie dans la synthèse supra.

Certes les ministères sont désormais plus nombreux à se doter de plans de renforcement de leur niveau de sécurité, en cohérence avec les politiques publiques qu'ils portent et traduisent les volontés ministérielles de se prémunir des principales menaces qui pèsent sur leurs activités mais ces plans d'actions restent à mettre en œuvre.

Le niveau effectif de conformité, qui fait l'objet d'un indicateur<sup>1</sup> 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.

### 3. L'engagement d'un travail interministériel de remédiation

**La refonte de la gouvernance SSI de l'Etat**, suivie dans le cadre du Comité de pilotage de la cybersécurité (COPIL Cyber) présidé par le cabinet du Premier ministre, a fait l'objet de travaux interministériels menés :

- d'une part, par l'ANSSI de septembre à décembre 2018 ;
- et d'autre part, par une mission d'inspection interministérielle de mars à juin 2019, dans la continuité de la mission d'inspection chargée de cartographier les ressources cybernétiques de l'Etat. Les rapporteurs de ces missions ont pu partager leurs constats avec ceux de la commission au cours de la mission d'information qu'ils ont conduite à la suite de la cyberattaque contre le système d'information « Ariane » du ministère de l'Europe et des affaires étrangères<sup>2</sup>.

**Les inspecteurs ont remis leur rapport fin mai 2019.** Celui-ci confirme la pertinence de l'organisation actuelle de la chaîne SSI ministérielle (prévue par la PSSIE) mais formule 21 propositions d'amélioration, en vue :

- d'assurer, au sein de chaque ministère, un pilotage au plus haut niveau de la politique SSI ;
- de poursuivre la responsabilisation des directions métiers et la sensibilisation de leurs dirigeants ;
- d'organiser la montée en compétence des responsables de la chaîne SSI notamment par la formation ;
- de créer une enceinte de gouvernance interministérielle présidée par le Premier ministre ou le Président de la République ;
- de formaliser les relations entre les ministères et l'ANSSI ;

---

<sup>1</sup> PLF 2020 PAP Mission Direction de l'action du Gouvernement programme 129, p. 30 et suiv. [https://www.performance-publique.budget.gouv.fr/sites/performance-publique/files/farandole/ressources/2020/pap/pdf/PAP20\\_20\\_BG\\_Direction\\_action\\_du\\_Gouvernement.pdf](https://www.performance-publique.budget.gouv.fr/sites/performance-publique/files/farandole/ressources/2020/pap/pdf/PAP20_20_BG_Direction_action_du_Gouvernement.pdf)

<sup>2</sup> [Rapport d'information n° 299 \(2018-2019\) de MM. Olivier Cadic et Rachel Mazuir](#)

- de réviser la PSSIE pour inscrire dans la norme cette nouvelle organisation.

#### **4. Une nouvelle feuille de route**

En conséquence, l'ANSSI a décliné ces propositions dans une feuille de route comprenant 13 actions dont vos rapporteurs ont pris connaissance. Ils partagent les objectifs et suivront avec attention la mise en œuvre.

Les premières actions, qui sont initiées depuis le mois de septembre 2019, consistent à la refonte de la « politique de sécurité des systèmes d'information de l'État » (PSSIE) afin :

- d'élaborer un texte de haut niveau visant à définir l'organisation et la gouvernance SSI applicable à l'ensemble des ministères ;
- de décliner des textes plus techniques, mis à jour plus régulièrement, pour y reporter et décrire les mesures opérationnelles et les méthodes de travail à mettre en œuvre ;
- de définir des indicateurs de mise en œuvre plus adaptés et pragmatiques afin de suivre l'évolution du niveau de sécurité global des ministères.

#### **5. Le nécessaire renforcement des moyens juridiques de l'ANSSI pour le contrôle des grands projets de l'Etat**

Actuellement, les moyens juridiques dont dispose l'ANSSI sont issus des dispositions des lois de programmation militaire, codifiées dans le Code de la défense, de la transposition en droit national de la directive *NIS*, de la compétence générale du secrétariat général de la défense et de la sécurité nationale en matière de conception des politiques de sécurité des systèmes d'information et du décret de création de l'agence.

Pour le contrôle des grands projets de l'État, l'ANSSI s'appuie désormais sur l'article 3 du décret du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique<sup>1</sup>.

##### **Observations sur le décret du 25 octobre 2019**

Ce texte soumet les projets interministériels et ministériels importants et les projets des organismes placés sous la tutelle de l'Etat à un avis du DiNum, conforme pour les premiers, simple pour les seconds. Ce dernier les transmet à l'ANSSI pour observations. Le DiNum peut demander les compléments d'information nécessaires à la formation de son avis ce qui suspend les délais d'instruction. A défaut, l'avis est réputé conforme.

<sup>1</sup> [Décret n° 2019-1088 du 25 octobre 2019 relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique](#)

Nous estimons souhaitable que les observations de l'ANSSI soient obligatoirement transmises aux administrations concernées, que le délai d'un mois soit interrompu par cette transmission et que la délivrance de l'avis conforme soit soumise à une appréciation par l'ANSSI de la qualité des réponses à ses observations.

S'agissant des opérateurs, la DInum n'a qu'un pouvoir de recommandations. Vos rapporteurs le regrettent car nombre de projets développés par les organismes placés sous la tutelle de l'Etat peuvent s'avérer sensibles et méritent une protection aussi importante que ceux des administrations. Un avis réservé de l'ANSSI devrait entraîner obligatoirement un nouvel examen.

Par ailleurs, au travers de la refonte de la PSSIE, l'ANSSI étudiera les possibilités de renforcer, de manière proportionnée, la contrainte pesant sur les services de l'Etat en vue de la bonne application des mesures prévues.

**La commission se réjouit de cette prise de conscience et des premières actions mises en œuvre, mais estime 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 de services de l'Etat sans se préoccuper suffisamment de leur sécurité et laisse perdurer des logiques de défenses des pré-carrés ministériels qui freinent encore ce qui devrait être une mobilisation générale contre des menaces croissantes et viennent retarder la mise en œuvre de mesures indispensables<sup>1</sup>.**

**Elle réitère son souhait que l'Etat fixe aux ministères la réalisation d'un ratio obligatoire d'investissement dans la cybersécurité assorti d'un système d'incitations/sanctions soit mis en place ; qu'une formation solide évaluée par l'ANSSI soit imposée pour tout recrutement des nouveaux DNum 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.**

---

<sup>1</sup> Le retrait du projet de décret relatif au système d'information et de communication de l'Etat et à la direction interministérielle du numérique, de la capacité pour le DInum de donner un avis aux ministres pour les nominations des directeurs numériques dans les ministères, au moins formellement, mesure sans doute symbolique, mais ô combien nécessaire, illustre parfaitement cette situation.

## C. 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<sup>1</sup>.

La directive européenne relative à la sécurité des systèmes d'information, dite NIS, transposée par une loi du 26 février 2018<sup>2</sup>, 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. La transposition de la « directive NIS »

L'enjeu de la directive<sup>3</sup> est d'assurer un niveau élevé et commun de sécurité dans l'UE<sup>4</sup>. Depuis sa transposition<sup>5</sup>, 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 élaborées par l'ANSSI.

Environ 120 opérateurs de services essentiels ont d'ores et déjà été désignés et une trentaine d'opérateurs sont en cours de désignation. Cette première vague de désignation a porté sur les opérateurs les plus importants pour le fonctionnement de l'économie ou de la société<sup>6</sup>.

La mise en œuvre de ces dispositions a eu pour principale conséquence organisationnelle d'élargir le nombre d'entités régulées et donc de provoquer un surplus d'activité, toutefois l'agence ne dispose pas d'une estimation des moyens budgétaires qui y ont été consacrés. Comme il a été exposé dans le précédent avis de la commission, **un renforcement des effectifs de l'ANSSI sera nécessaire pour se saisir des nouvelles prérogatives. Le retour à une progression du schéma d'emplois de 50 ETP par an au cours des prochaines années satisfait cette observation.**

---

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (dite « directive NIS »).

<sup>4</sup> Sénat [n° 110 Tome IX \(2017-2018\) par MM. Cadic et Mazuir p. 33 et suiv.](#)

<sup>5</sup> Loi n° 2018-133 du 26 février 2018.

<sup>6</sup> De ce fait, une majorité de ces opérateurs sont des opérateurs d'importance vitale et donc déjà soumis aux dispositions en matière de cybersécurité instaurées par l'article 22 de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019.

## 2. La protection des réseaux

La sécurisation des réseaux de télécommunications est un enjeu majeur. L'ANSSI joue un rôle central dans le contrôle réglementaire instauré en application de l'article 226-3 du code pénal qui soumet à autorisation la commercialisation et la détention d'équipements susceptibles de porter atteinte à la confidentialité des communications électroniques<sup>1</sup>.

**La loi n° 2019-810 du 1<sup>er</sup> août 2019** visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux électriques mobiles introduit une obligation d'autorisation préalable, par le Premier ministre, de l'exploitation des appareils d'infrastructure des réseaux mobiles de 5<sup>ème</sup> génération qui présentent, par leur fonctionnalité, un risque pour la sécurité de ces réseaux<sup>2</sup>. L'ANSSI assurera effectivement, en lien étroit avec le SGDSN, l'instruction technique et administrative des demandes d'autorisation découlant de ce nouveau régime. Ce dispositif vient donc compléter le dispositif existant<sup>3</sup>. Elle dispose déjà d'un savoir-faire et d'une expérience significative dans l'analyse de tels équipements, et dans la mise en œuvre d'un régime de contrôle réglementaire, qu'elle transposera dans le traitement du nouveau régime d'autorisation préalable.

Même si les champs d'application des deux régimes ne sont pas strictement équivalents il est anticipé à terme une volumétrie d'autorisations L. 34-11 d'au plus un millier de demandes par an, laquelle devrait s'établir progressivement, à compter des premiers déploiements de la 5G attendus en 2020<sup>4</sup>.

---

<sup>1</sup> 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 5<sup>ème</sup> génération.

<sup>2</sup> Article 34-11 du code des postes et des communications électroniques (CPCE). Voir sur ce point [l'avis n° 569 \(2018-2019\)](#) de M. [Pascal Allizard](#) au nom de la commission des affaires étrangères, de la défense et des forces armées du Sénat.

<sup>3</sup> En particulier le régime de contrôle», découlant des articles 226-3, R. 226-3 et R. 226-7 du Code pénal qui soumet à autorisation la commercialisation (R. 226-3) et la détention (R. 226-7) de tout dispositif de nature à permettre une atteinte au secret des correspondances électroniques ou à la vie privée, parmi lesquels figurent de nombreux équipements d'infrastructure des réseaux mobiles. Ce contrôle R. 226 donne actuellement lieu, dans sa globalité, à la délivrance d'environ 1 200 autorisations par an, réparties équitablement entre autorisations de commercialisation R. 226-3 (664 autorisations en 2018) et autorisations de détention R. 226-7 (602 autorisations en 2018). Parmi ces dernières, environ 500 portent sur des équipements du domaine des télécommunications, le reste relevant principalement des différents types d'outils d'investigation numérique et de techniques de renseignement prévus par la loi.

<sup>4</sup> Dans la mesure où ces déploiements ne porteront initialement que sur les « antennes » 5G, et non sur les infrastructures centrales dites de « cœur de réseau » (déploiement 5G dit « non standalone », dans lequel le cœur de réseau reste en technologie 4G), alors que ces cœurs de réseau représentent une part importante de la typologie d'appareils soumis à autorisation.

L'ANSSI prévoit d'assurer le traitement de ces demandes selon la même logique que les demandes R.226, avec des personnels consacrés à l'instruction administrative, s'appuyant en tant que de besoin sur des expertises techniques fournies par d'autres équipes de l'ANSSI dont le renforcement a été anticipé. Afin de faire face à la volumétrie à terme, mais également à un niveau d'exigence renforcé sur les délais<sup>1</sup>, deux ETP complémentaires seront affectés au traitement administratif des nouvelles demandes. Par conséquent, la mise en œuvre de ces nouvelles dispositions devrait pouvoir être assurée sans moyens complémentaires.

Enfin, un bilan de la première année de mise en œuvre de ces nouvelles dispositions sera intégré au rapport annuel que le gouvernement remettra au Parlement à compter du 1<sup>er</sup> juillet 2020, comme le prévoit l'article 5 de la loi.

#### ***D. L'ANSSI, ACTEUR DE LA CONSOLIDATION DE LA FILIÈRE FRANÇAISE DE SÉCURITÉ INFORMATIQUE***

Le volet financement, reposant, d'une part, sur des appels à projets du Programme d'investissements d'avenir et, d'autre part, sur une convention entre Bpifrance et l'ANSSI, a ainsi permis de soutenir le développement de solutions nationales de détection d'attaques informatiques qualifiées en avril 2019. Par ailleurs, la société d'investissement ACE Management a réalisé cette année le *closing* de son nouveau fonds Brienne III, premier fonds français entièrement voué à la cybersécurité, pour un montant de 80 M€.

Une nouvelle étape dans la consolidation de la filière des industries de sécurité a été franchie en novembre 2018 avec sa labellisation dans le cadre du Conseil national de l'industrie<sup>2</sup>.

En complément, une mission a été confiée par le Premier ministre à Michel Van Den Berghe, directeur général d'Orange Cyberdéfense, pour la préfiguration d'un « **campus de la cybersécurité** », afin de réunir et renforcer l'ensemble des acteurs de l'écosystème français. En tant qu'acteur central de l'écosystème de la cybersécurité en France, l'ANSSI s'investit pleinement dans ce projet. Ce campus vise à répondre à trois grands enjeux :

- renforcer sensibilisation et formation pour contribuer à résoudre le déficit d'experts et renforcer la prise en compte du risque dans les organisations ;

---

<sup>1</sup> Les autorisations L.34-11 doivent être accordées ou refusées dans un délai de deux mois à compter de la réception d'un dossier de demande complet, délais inférieurs à ceux généralement constatés sur les autorisations R.226.

<sup>2</sup> Un contrat de filière qui doit être signé avant fin 2019 avec le comité stratégique de filière (CSF). Il comportera cinq projets structurants, qui seront soutenus par des engagements forts de l'industrie comme de l'Etat : Jeux Olympiques de Paris en 2024 ; Territoires de confiance ; Identité numérique ; Cybersécurité et sécurité de l'IoT ; Numérique de confiance.



- favoriser partage et mutualisation d'outils, de compétences et de données entre acteurs de l'écosystème ;
- accompagner l'innovation publique et privée pour concourir au développement de la filière industrielle de cybersécurité, en cohérence avec le comité stratégique de filière sécurité.

#### IV. 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. L'ACCROISSEMENT DE SON ACTIVITÉ

**La progression de l'activité est considérable** en raison de l'encadrement, depuis l'entrée en vigueur des lois de 2015, de techniques dont l'usage se répand dans les services spécialisés. Elle résulte également de l'intensification de la lutte contre le terrorisme, priorité affichée depuis les attentats de 2015.

De 2017 à 2018, le recours aux techniques de renseignement a encore considérablement augmenté :

- dans des proportions de l'ordre de 20 à 25 % selon les techniques, y compris pour celles qui étaient encadrées avant 2015 (interceptions de sécurité, relevés de communications, identifications) ;
- le nombre de réquisitions adressées par le GIC aux opérateurs a augmenté de 30 % ;
- le nombre de transcriptions contrôlées par le GIC a augmenté de 25 % ;
- le nombre de mesures de surveillance internationale a augmenté de 40 %.

### Nombre d'avis préalable rendus par la CNCTR

<b>Techniques de renseignement (articles du Code de la sécurité intérieure)</b>	2016	2017	2018	Évolution 2018/2017
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	28 741	-4,6%
Accès aux données de connexion en temps différé (art. L. 851-1) (autres demandes dont celle de factures détaillées)	15 021	18 512	17 443	- 5,8%
Géolocalisation en temps réel (art. L. 851-4)	2 426	3 751	5 191	+38,4%
Interceptions de sécurité (art. L. 852-1 I)	8 137	8 758	10 562	+20,6%
Autres techniques de renseignement <sup>1</sup>	9 408	9 295	11 361	+4,1%
<b>Ensemble des techniques de renseignement</b>	<b>67 088</b>	<b>70 432</b>	<b>73 298</b>	<b>+4,1%</b>

Source : CNCTR – 3<sup>e</sup> Rapport d'activité novembre 2018.

#### **B. 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<sup>2</sup>, mais aussi aux demandes spécifiques du Premier ministre ou de l'autorité de contrôle pour la supervision de l'activité des services. En 2020, l'actualisation de certaines dispositions de la loi de 2015 pourrait conduire à de nouvelles adaptations rendant nécessaires de nouveaux développements informatiques.

- 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 (voir infra p. 36).

<sup>1</sup> 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).

<sup>2</sup> Sénat [n° 149 Tome IX \(2018-2019\)](#) par MM. Cadic et Mazuir p. 39 et suiv.

## TITRE 2 : LES MOYENS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2020

Le budget opérationnel du programme du SGDSN dans le projet de loi s'élève à 311 M€ en AE (**310,3 M€ en 2019**) en AE et 277,5 M€ en CP (**293,9 M€ en 2019**) et le **plafond d'emplois à 1 267 ETPT (1 216 en 2019)**.<sup>1</sup>

### CRÉDITS DU BOP SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2020

(EN MILLIONS D'€)

	Exécution 2018		LFI 2019		PLF 2020	
	AE	CP	AE	CP	AE	CP
<i>Titre 2</i>	84,5	84,5	97,2	97,2	80,1	80,1
<i>HT2</i>	94,2	90,6	213,1	196,7	230,9	197,4
<b>TOTAL</b>	<b>178,7</b>	<b>175,1</b>	<b>310,3</b>	<b>293,9</b>	<b>311</b>	<b>277,5</b>

*L'écart entre l'exécution 2018 et la budgétisation 2019/2020 s'explique, comme tous les ans en HT2 par d'importants volumes de transferts de crédits vers différents ministères, notamment au titre des capacités techniques interministérielles et du développement de produits de sécurité nationaux. En T2, elle s'explique par la décision de ne plus procéder, à compter de 2020, au remboursement des personnels mis à disposition du SGDSN par le ministère des armées, au titre de la participation de ce ministère à la coordination de la sécurité et de la défense nationale et au renforcement de la cyberdéfense.*

L'évolution des crédits recouvre des évolutions contrastées :

- une augmentation de **33 M€** en AE des crédits **hors titre 2** de l'ANSSI pour couvrir le renouvellement du bail de la Tour Mercure ;
- une augmentation de **3 M€ en AE=CP** au titre de l'actualisation des capacités techniques interministériels ;
- une diminution de **14,7 M€** de crédits de **titre 2** (dont 7,1 M€ au titre des crédits CAS « Pensions ») contraction d'une hausse liée aux créations d'emplois et d'une baisse liée à la décision de ne plus procéder au remboursement, à compter de 2020, des rémunérations des personnels militaires affectés temporairement au SGDSN par le ministère des Armées au titre de la participation de ce ministère à la coordination de la sécurité et de la défense nationale et au renforcement de la cyberdéfense, actuellement au nombre de 254 (SGDSN : 33, ANSSI : 41, CTG : 151, GIC : 29). Leur statut restera inchangé en 2020.

**Ce transfert de charges porte sur un montant évalué sur la base 2019 à 22,38 M€ (dont 9,54 M€ au titre du CAS Pensions).** Seules les primes spécifiques versées à ses militaires au titre de leurs affectations temporaires resteront à la charge du titre 2 du programme 129 pour un montant de 0,445 M€.

<sup>1</sup> Le BOP SGDSN recouvre les crédits destinés à l'ensemble SGDSN/ANSSI placés sous l'autorité du SGDSN 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.

### *Observations générales des rapporteurs*

#### **1. La présentation des crédits du SGDSN et des entités qui en dépendent : un effort de précision dans la présentation reste à réaliser**

A l'inverse du GIC, service à compétence nationale<sup>1</sup>, 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 plus de 60% des effectifs budgétaires (650/1027 ETP), et le tiers des crédits de l'unité opérationnelle SGDSN (opérateurs compris) et relève du même statut juridique<sup>2</sup>, 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 et dans la ventilation des emplois 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 cybersécurité et à la bonne information du public. Vos rapporteurs ne rencontrent pourtant aucun obstacle à obtenir ces informations du SGDSN.*

*Les dispositions arrêtées pour permettre une présentation des dépenses de fonctionnement de l'ensemble SGDSN/ANSSI et notamment de l'expérimentation d'un tableau de bord budgétaire élaboré par entités et directions soutenues (AIST, ANSSI, CTG, PSE, SAG, Opérateurs, INFRA) répondent à la recommandation formulée depuis plusieurs années par la commission. Il serait souhaitable que ce travail permette une documentation plus précise dans le PAP et dans de RAP.*

#### **2. La prise en charge des crédits de Titre 2 concernant la rémunération des personnels militaires en fonction au SGDSN et dans les entités qui en dépendent par la Mission Défense ne permet pas d'apprécier de façon transparente le coût de l'activité du SGDSN et de ces entités.**

Même si elle repose sur un amendement aux conventions entre le Ministère des Armées et le SGDSN, cette décision paraît contraire à l'esprit de la loi organique relative aux lois de finances (LOLF), et notamment de son article 7, selon lesquelles : « une mission comprend un ensemble de programmes concourant à une politique publique définie » et « un programme regroupe les crédits destinés à mettre en œuvre une action ou un ensemble cohérent d'actions relevant d'un même ministère et auquel sont associés des objectifs précis, définis en fonction de finalités d'intérêt général, ainsi que des résultats attendus et faisant l'objet d'une évaluation ». L'exclusion du Titre 2 du programme 129, de la rémunération des personnels militaires concourant à la politique interministérielle de coordination de la sécurité et de la défense et donc de la coordination du travail gouvernemental placé au sein de la mission de direction de l'action du gouvernement confiée au Premier ministre, ne permet plus à la représentation nationale d'apprécier dans leur entièreté les moyens mis en œuvre au service des actions engagées et d'en évaluer la performance.

*Il serait souhaitable que le Premier ministre revienne sur cette décision et à défaut à la ministre des Armées et au ministre du budget de créer un article spécifique dans le programme 212 pour retracer les crédits dépensés par les Armées pour solder les personnels militaires affectés au SGDSN et au sein des entités qui en dépendent.*

<sup>1</sup> Décret n° 2016-1772 du 20 décembre 2016.

<sup>2</sup> Décret n° 2009-834 du 7 juillet 2009 modifié.

## 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 +55 ETP (dont +42 pour l'ANSSI, +15 GIC) a été accordé en PLF 2020 pour l'ensemble du SGDSN (action 2), faisant passer le plafond d'emplois de 1 216 ETPT en LFI 2019 à 1 267 ETPT en PLF 2020.

EFFECTIFS DU SGDSN DANS LE PROJET DE LOI DE FINANCES POUR 2020

	LFI 2019		PLF 2020	
	ETP (schéma d'emplois)	ETPT	ETP (schéma d'emplois)	ETPT
ANSSI	+42		+42	
CTG				
SGDSN hors ANSSI et CTG	-5			
Total SGDSN	+37	988		1 027
GIC	+15	228	+13	240
BOP SGDSN	+52	1 216	+55	1 267

Source : SGDSN / Réponse au questionnaire budgétaire.

Sous réserve de la consolidation des crédits du titre 2, l'estimation de la masse salariale du SGDSN en 2020 est de 80,1 M€ (97,2 M€ en 2019, dont 18,63 M€ sur le CAS Pensions). Cette baisse de 17,7 % s'explique essentiellement par<sup>1</sup> :

- le schéma d'emplois de l'ANSSI (+42 ETP) et du GIC (+13 ETP), représentant au total 55 ETPT sur le plafond d'emplois ;

- une diminution de 17,2 M€ de crédits de **titre 2 (dont 14,7 M€ pour le SGDSN/ANSSI et 2,4 M€ pour le GIC)** dont 8,7 M€ (dont 7,1 M€ pour le SGDSN/ANSSI et 1,6 M€ pour le GIC) au titre des crédits CAS « Pensions », liée à la décision de ne plus procéder au remboursement, à compter de 2020, des rémunérations des personnels militaires affectés temporairement au SGDSN par le ministère des Armées (*voir supra p.27*).

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

Le SGDSN devrait maintenir ses effectifs en 2020 après plusieurs années de diminution.

---

<sup>1</sup> Elle conduira à un plafond d'emplois à l'échelle du SGDSN de 1 191 ETPT.

### **C. L'ANSSI : UNE NÉCESSAIRE REMONTÉE EN PUISSANCE DES EFFECTIFS**

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 liée à la numérisation croissante des activités humaines. L'effort en faveur de la croissance des effectifs de l'agence sera poursuivi en 2020, compte tenu de la croissance de la charge de ses missions habituelles et de l'attribution de nouvelles missions (voir supra p.22).

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<sup>1</sup>. En 2018, de fait en raison d'une sous-évaluation des crédits inscrits en titre 2<sup>2</sup>, il n'a pu être procédé qu'à 8 créations de postes. Les 17 postes ont été pourvus en 2019 et se sont ajoutés au 25 ETP dont la création était prévue dans le schéma d'emplois.**

**Un nouvel arbitrage a été rendu pour maintenir à 42 le nombre de créations en 2020, avec la perspective de revenir à 50 en 2021 et 2022. Ainsi le schéma d'emploi de l'ANSSI atteindra 635 ETPT en fin d'année 2020, ce dont vos rapporteurs ne peuvent que se réjouir compte tenu de l'accroissement des missions de l'ANSSI (voir infra) et atteindre 681 ETPT en fin d'année 2021.**

Dans son précédent avis, la commission avait noté que l'agence est confrontée à la rareté des ressources humaines de haut niveau dans certaines spécialités<sup>3</sup>. Ce constat partagé avait conduit à mettre en place un plan d'action pour attirer et fidéliser les agents exerçant ces métiers<sup>4</sup>.

---

<sup>1</sup> Dans leur avis budgétaire sur le PLF 2018, s'étaient inquiétés du choix de réduire de 50 à 25 ETP la progression annuelle du schéma d'emplois de l'ANSSI compte tenu des enjeux. Avis Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 50.

<sup>2</sup> 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 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.

<sup>3</sup> Avis Sénat n° 110 Tome IX (2017-2018) par MM. Cadic et Mazuir p. 44 et suiv.

<sup>4</sup> 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.

#### **D. LE GIC : GARDER LA MAÎTRISE DES EFFECTIFS ET ASSURER LEUR MONTÉE EN PUISSANCE**

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

	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).

**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<sup>1</sup>.**

**Les retards accumulés en 2017 (10 ETP) n'ont pas pu être comblés en 2018 et se sont même accrus<sup>2</sup>. La situation s'est stabilisée, le GIC dispose d'un schéma d'emplois de +15 ETP et ses effectifs devraient atteindre 190,5 ETP fin 2019, soit un décalage de 39,5 ETP par rapport au schéma initial, avec une masse salariale correspondante de 13,7 M€. Pour 2020, il est prévu 13 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 depuis 2017.**

**Il convient de se féliciter de cette adaptation aux besoins en construction budgétaire. L'objectif est d'atteindre une cible de 243 ETPT à l'horizon 2021. Reste cependant à le réaliser, d'autant que l'activité du GIC se développe (voir supra p. 25).**

Les crédits inscrits dans le PLF 2020 au titre 2 de l'unité opérationnelle GIC s'élèvent à 11,38 M€ (13,8 M€ en PLF 2019 ; 12,6 M€ en PLF 2018 et 10,9 en PLF 2017), soit une baisse de 17,5%.

En effet, pour les raisons indiquées (voir supra p. 27), il a été décidé de ne plus procéder au remboursement, à compter de 2020, des rémunérations des personnels militaires mis à disposition du GIC par le ministère des Armées au titre de la participation de ce ministère à la coordination de la sécurité et de la défense nationale à partir de l'année 2020, soit une non imputation de **2,4 M€** dont 1,6 M€ au titre des crédits CAS « Pensions ». Ces montants correspondent à un effectif de 36 militaires

<sup>1</sup> Exprimé en ETPT, cela porte le plafond d'emplois à 213 ETPT en LFI 2018 et à 228 en PLF 2019.

<sup>2</sup> En 2018, les effectifs du GIC devaient progresser par un schéma d'emplois de +15 ETP. Les difficultés de recrutement, liées notamment aux délais d'habilitation au secret de la défense nationale des personnels, à de nombreux départs en fin d'année et au manque de postes de travail disponibles dans une partie des structures du GIC ont conduit à un schéma d'emploi de -8 ETP. Les effectifs du GIC, sur le périmètre du SGDSN, ont donc baissé à 175,5 ETP fin 2018, soit un décalage de 40 ETP par rapport au schéma initial. La masse salariale correspondante consommée en 2018 est de 12,17 M€.

actuellement en fonction (pour 44 emplois ouverts dans le schéma d'emploi du GIC).

A contrario, ces crédits sont majorés de 868 400 €<sup>1</sup> au titre du transfert de crédits correspondant à l'imputation directe au programme 129 de 10 ETPT (gendarmes mis à disposition du SGDSN au profit du GIC jusqu'ici pris en charge par le programme 152, gendarmerie nationale de la Mission Sécurité intérieure). Il a été décidé que ces gendarmes (à l'instar des 9 postes créés en loi de finances pour 2017), seraient affectés avec remboursement des rémunérations par l'organisme d'affectation. Il sera ainsi procédé par imputation directe sur les crédits du programme 129.

**La première opération ne permet plus d'évaluer le coût réel des charges de personnels du GIC. En revanche, la prise en compte des charges de personnel nécessaire à la sécurisation des enceintes du GIC par la Gendarmerie nationale est une décision positive pour cette appréciation. Le caractère contradictoire de ces dispositions doit être relevé. Elles obéissent semble-t-il davantage à des choix d'opportunités qu'à une logique budgétaire bien arrêtée dans l'esprit de la LOLF.**

Dans leur précédent avis<sup>2</sup>, la commission avait mis en exergue les freins au recrutement et identifié des axes de progression. **Des mesures ont été prises pour diversifier les modes de recrutement en 2019 mais leur rythme de mise en œuvre devra être accéléré pour atteindre l'objectif à l'horizon 2021 avec l'ouverture d'une nouvelle implantation immobilière.**

La commission maintient ses observations. Elle estime que les règles de recrutement des contractuels devraient être assouplies dans certaines situations, tant dans la définition des plafonds de rémunération que pour l'accélération des procédures de recrutement. La transformation et la modernisation du GIC est 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 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 2020 prévoit l'ouverture de 213,97 M€ d'AE (196,08 M€ en 2019) et de 180,46 M€ de CP (179,7 M€ en 2019) pour l'ensemble SGDSN/**

---

<sup>1</sup> 450 600 € hors CAS pensions et 417 800 € au titre du CAS pensions.

<sup>2</sup> [Sénat n° 149 Tome IX \(2018-2019\) par MM. Cadic et Mazuir p. 48 et suiv.](#)



ANSSI (hors GIC et subvention aux opérateurs). Cela représente, en CP, **une évolution de l'ordre de 9 % en AE et de 0,5 % en CP par rapport à la LFI 2019**. Les crédits ouverts seront essentiellement mobilisés pour le développement des capacités techniques interministérielles liées à la sécurité nationale. L'écart entre CP et AE est en grande partie imputable aux engagements (33 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 (63,22 M€ en CP et 63,73 M€ en AE) est en baisse par rapport à 2019 (79,38 M€ en CP et 94,74 M€ en AE).**

**Hors ANSSI, le SGDSN dispose de 96,05 M€ en CP pour 2020, et de 137,16 M€ en AE.** 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 7,80 M€ en 2020 en CP. 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 dont une large partie est transférée en cours d'exercice vers le ministère de la défense dont l'enveloppe augmente sensiblement.

## **2. Crédits de fonctionnement de l'ensemble SGDSN/ANSSI (hors GIC et subvention aux opérateurs)**

**Dans le Projet annuel de performances<sup>1</sup>, les crédits de fonctionnement du SGDSN sont évalués à 88,7 M€ en AE et 55,3 M€ en CP pour 2020. Ils sont destinés à couvrir principalement les dépenses suivantes :**

- le fonctionnement des systèmes d'information sécurisés, leur maintien en condition opérationnelle et le transfert de compétence nécessaire à leur utilisation (17,6 M€ en AE et 15,8 M€ en CP) ;
- la politique d'expertise scientifique et technique et le développement des produits de sécurité ( 8 M€ en AE et 7,1 M€ en CP) ;
- les dépenses immobilières pour les sites de l'Hôtel national des Invalides, de la Tour Mercure, du Fort du Mont-Valérien et de la zone de stockage de Pantin<sup>2</sup> (3,9 M€ en AE et 9,5 M€ en CP) ainsi que le renouvellement du bail du bâtiment Mercure : 33 M€ en AE en 2020 ;

---

<sup>1</sup> [Projet annuel de performances p. 65](#)

<sup>2</sup> 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.

### **La satisfaction des besoins immobiliers de l'ANSSI : une priorité**

Dans son précédent avis, la commission avait souligné que le cadre de travail constituait un déterminant important dans le choix des candidats sur des marchés en tension.<sup>1</sup>

Les moyens techniques et humains de l'ANSSI sont aujourd'hui répartis, à Paris, entre l'Hôtel national des invalides (propriété de l'Etat) et la Tour Mercure (propriété de la Société Aviva). S'y ajoutent deux sites à vocation purement technique n'hébergeant que très peu de personnel permanent, que sont le centre de données et un centre de logistique et de stockage implantés tous deux en région parisienne.

L'organisation immobilière actuelle ne permettra pas d'absorber l'accroissement prévisionnel des effectifs de l'ANSSI de l'ordre de 50 ETP par an. Dans ce contexte, il a été décidé d'une part de prolonger le bail de la Tour Mercure et, d'autre part, d'ouvrir une antenne de l'ANSSI à Rennes, à proximité du pôle cyber du ministère des armées. 200 ETP devraient y être installés à l'horizon 2025.

Enfin, le projet de création d'un grand campus ayant vocation à soutenir et à fédérer les acteurs du numérique et de l'innovation autour des enjeux de la cybersécurité pourrait potentiellement avoir des effets sur les implantations de l'ANSSI.

### **3. Les dépenses d'investissement**

**Dans le Projet annuel de performances<sup>2</sup>, 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. Les dépenses d'investissement prévues pour 2020 sont évaluées à 107,9 M€ en AE et 108,2 M€ en CP et ont vocation à financer principalement les projets suivants<sup>3</sup> :**

- **gestion des capacités informatiques du SGDSN et déploiement et à l'administration des moyens et des services de l'ANSSI pour l'ensemble de ses projets internes et externes (22,2 M€ en AE et 20,5 M€ en CP) ;**

- **poursuite des travaux immobiliers déjà engagés (8 M€ en AE et 9 M€ en CP) : sécurisation des accès et de la distribution électrique, rénovation du système de sécurité incendie et durcissement de la protection du centre de transmission gouvernemental (CTG), remplacement des installations de production de froid et augmentation de la capacité de dévolution du CTG aménagement d'une zone logistique pour l'ANSSI ;**

- **projets interministériels liés à la défense et à la sécurité nationale dans le cadre des capacités techniques interministérielles (70 M€ en AE et CP).**

<sup>1</sup> [Sénat n° 149 Tome IX \(2018-2019\)](#) par MM. Cadic et Mazuir p. 46 et 47.

<sup>2</sup> [Projet annuel de performances p.67](#)

<sup>3</sup> *Pour l'ANSSI, les dépenses d'investissement financent, d'une part, ses missions d'expertise, en particulier, les besoins des administrations en logiciels et services de sécurité et, d'autre part, la sécurité des systèmes d'information ;*

#### 4. Les dépenses d'intervention

Le SGDSN a prévu une dotation de 4 M€ en AE et 3,6 M€ en CP pour les dépenses d'intervention dont principalement : 2 M€ en AE et 1,8 M€ en CP ont vocation à financer des actions en matière de sécurité des systèmes d'information, que ce soit dans le cadre d'une convention relative à la cybersécurité des systèmes du futur, dans le cadre de la convention avec BPI France, ou dans le cadre de groupements d'intérêt public notamment (GIP dédié au développement et à la promotion des entreprises, GIP pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance).

#### B. LE MAINTIEN DE L'EFFORT BUDGÉTAIRE POUR ACCOMPAGNER L'ACTIVITÉ DU GIC

##### Évolution des crédits consacrés au GIC depuis 2017

*En millions d'euros*

	2017		2018		2019		2020	
	AE	CP	AE	CP	AE	CP	AE	CP
LFI et PLF	15,61	15,61	15,59	15,59	16,97	16,98	16,97	16,98
Exécution		12,17		16,68				

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 2020, le budget HT2 en fonds normaux du GIC, **16,97 M€ en AE et 16,98 M€ en CP** (stable par rapport à 2019) 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 récemment acquis.

#### 1. Les crédits de fonctionnement

Les crédits de fonctionnement courant 8,3 M€ en AE et CP en 2020 (7,2 M€ en AE et en CP en 2019, 4,8 en AE et 3,5 en CP en 2018) ont vocation à financer le fonctionnement et le maintien en conditions opérationnelles des différents systèmes d'information et réseaux existants, ainsi que le raccordement au réseau interministériel de l'État. Ces crédits couvrent 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 2,7 M€ en AE et CP (1,7 M€ en AE et en CP en 2019, 1,4 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.

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 2020, les dépenses d'investissement prévues sont de 8,7 M€ en AE et CP (9,8 M€ en AE et en CP en 2019, 10,8 en AE et 12,2 en CP en 2018) et se répartissent en :**

- des dépenses pour immobilisations incorporelles pour 4,4 M€ en AE et CP (5 M€ en AE et en CP en 2019, 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 réglementaire depuis 2015 ;
- des dépenses pour immobilisations corporelles à hauteur de 3,3 M€ en AE et CP (comme en 2019, 4,3 M€ en AE et 5,9 en CP en 2018) qui concernent notamment l'achat d'équipements pour la réalisation d'un système de développement et de recette, l'extension des réseaux informatiques et l'équipement d'un centre de données dans le nouveau site.
- des dépenses liées à des travaux immobiliers réalisés dans l'immeuble en cours d'acquisition pour 1 M€ en AE et CP.

### **La satisfaction des besoins immobiliers du GIC : une opération en cours**

Les implantations parisiennes actuelles sont devenues insuffisantes pour faire face à la croissance des effectifs du GIC et des sections des services exploitant sur place.

**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 a été réalisée à la fin de l'année 2018, financée sur les crédits du compte d'affectation spéciale « gestion du patrimoine immobilier de l'État ». La majeure partie des aménagements sera financée sur ce même CAS ; le solde sur les crédits du programme 129. Le nouveau bâtiment ouvrira ses portes en 2021 à la suite de travaux importants permettant notamment l'installation d'un centre de données.**

### III. LES FONDS SPÉCIAUX : DES CRÉDITS EN CROISSANCE

Les fonds spéciaux, consacrés au financement de diverses actions liées à la sécurité extérieure et intérieure de l'État, s'élèvent à 76,8 M€ en AE en AE et CP dans le PLF 2020<sup>1</sup>, un montant en croissance par rapport à celui inscrit en LFI 2019 (66,8 M€).

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 au sein du P129 (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	8 840 000	9 220 000	3 119 759	88 370 100
2019	66 804 810	13 640 000	4 800 000	-	
2020*	76 804 810				

\*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*

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, souligné dans ses précédents rapports par la CVFS, a été limité depuis 2015<sup>2</sup>. Pour autant, la CVFS observait, dans son rapport sur les crédits de 2016<sup>3</sup>, 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.

**La commission s'était associée à cette recommandation. L'accroissement du montant des crédits dans le PLF 2020 laisse entrevoir que celle-ci a été au moins partiellement prise en compte.**

<sup>1</sup> Source : projet annuel de performances.

<sup>2</sup> [Rapport de la délégation parlementaire au renseignement pour 2017](#) p.68

<sup>3</sup> 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) et l'Institut national des hautes études de la sécurité et de la justice (INHESJ).

Depuis 2017, le développement de leur activité est inscrit dans un contexte de stabilisation des subventions pour charges de service public et des emplois, et de mutualisation de certaines de leurs activités et structures.

**Pour 2020 les subventions et les plafonds d'emploi des deux instituts sont en diminution :**

- pour IHEDN à 7,3 M€ en AE et en CP et 88 ETPT (7,6 M€ en AE et en CP et 92 ETPT en 2019) ;
- pour INHESJ à 6,1 M€ en AE et en CP et 78 ETPT<sup>1</sup> (6,2 M€ en AE et en CP et 73 ETPT en 2019).

La circulaire du Premier ministre du 5 juin 2019 sur la transformation des administrations centrales et les nouvelles méthodes de travail invite à simplifier les structures administratives en examinant notamment le maintien des structures et opérateurs de moins de 100 ETP. Les deux opérateurs étaient potentiellement concernés par cette circulaire. Une réflexion a été, en conséquence, engagée par les services du Premier ministre qui porte notamment sur les entités pour lesquelles existent dans les ministères des structures intervenant sur les mêmes missions.

**Il a été dès lors considéré que l'INHESJ, pour laquelle des formations sont mises en place dans les ministères concernés comme avec le cycle supérieur d'administration de la justice ou les formations mises en place par le centre des hautes études du ministère de l'intérieur, pouvait être supprimée et ses activités réparties entre des structures existantes. Cette suppression au 31 décembre 2020 a été confirmée par la Premier ministre le 8 octobre 2019.**

S'agissant de l'IHEDN, structure plus ancienne, le caractère interministériel de ses activités a été réaffirmé et sa pérennité dans le périmètre des services du Premier ministre assurée, sous réserve d'une évolution de son offre de formation. La défense nationale<sup>2</sup> englobe des problématiques qui vont au-delà de la seule défense militaire. Une mission a été confiée en ce sens au directeur de l'Institut, le Général Destremau.

---

<sup>1</sup> (71 sous plafond et 7 hors plafond dont 6 apprentis).

<sup>2</sup> Dans la logique de l'ordonnance n° 59-147 du 7 janvier 1959 portant organisation générale de la défense et du code de la défense.

## 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 2020-2022 qui n'est toujours pas adossé à un contrat d'objectifs et de performances

Le Plan Stratégique IHEDN 2020<sup>1</sup> adopté en novembre 2015, n'avait pas été suivi de la conclusion entre l'établissement public et sa tutelle d'un contrat d'objectifs et de performances 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. Une remise en mouvement de la démarche stratégique et, de façon concomitante, la conclusion d'un contrat d'objectifs et de performances comprenant les indicateurs pertinents était attendue de la direction de l'Institut et du SGDSN.

**Un nouveau plan stratégique 2019-2022 a été présenté** qui prévoit le resserrement de l'offre de formation « *sur l'essentiel pour mieux répondre aux besoins de l'État et de la Nation, ainsi qu'aux attentes de ses auditeurs, de ses prescripteurs et de l'ensemble des parties prenantes* », tout en amorçant « *une rénovation profonde visant à bâtir un Institut de formation stratégique de référence pour l'État et en Europe* ».

**Ce plan (2020-2022) dont on doit souligner la qualité de la présentation et de la réflexion sous-jacente s'articule autour de quatre axes, déclinés en 10 objectifs et en 50 actions qui concernent toutes les missions fondamentales de l'Institut.**

#### Les 4 axes du plan stratégique

- Assurer en priorité la qualité d'une offre de formation recentrée et d'études visant l'excellence ;
- Attirer et fidéliser des hauts potentiels ;
- Contribuer au développement de la réflexion stratégique, tout en favorisant un travail prospectif, axe majeur pour un Institut situé au croisement d'un large réseau d'expertises et de savoirs, en vertu de son positionnement interministériel ;
- Améliorer le modèle économique dans un cadre budgétaire contraint.

<sup>1</sup> [http://issuu.com/ihedn/docs/plan\\_strat\\_gique\\_ihedn\\_2020\\_web/1?e=4027381/33785420](http://issuu.com/ihedn/docs/plan_strat_gique_ihedn_2020_web/1?e=4027381/33785420)



Un processus de pilotage de la transformation a été mis sur pied pour assurer le bon avancement des travaux qui s'échelonnent jusqu'à l'été 2021.

**Il reste que ce plan stratégique qui comprend un contrat d'objectifs et de performances ne contient aucune programmation budgétaire et financière, ce qui constitue une faiblesse intrinsèque et ne permet pas d'en apprécier la soutenabilité. Des arbitrages politiques restent à rendre.**

## 2. Les activités de l'IHEDN

Selon le rapport d'activité de l'Institut, l'année 2018 a vu augmentation de 25,6 % du nombre de journées de formation/auditeurs-participants qui passe de 27 769 en 2017 à 34 897.

Les formations stricto sensu représentent près de 80,7% de l'activité. Les formations au niveau national 74,7%: les sessions nationales (*politique de défense, armement et économie de défense, enjeux maritimes*) 26,6%, les séminaires jeunes plus de 14,4% et les sessions en région près de 26,1%.

Les sessions « jeunes » et en région progressent très sensiblement<sup>1</sup>. Un effort a été produit sur les journées d'information et colloque<sup>2</sup>. L'année 2019 s'est inscrite dans la continuité de 2018 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 dont une première session a accueilli 40 auditeurs, l'organisation de deux sessions « *enjeux maritimes* », de 16 cycles jeunes, d'une vingtaine de formations « *Intelligence économique et Cyberdéfense* », de 3 formations au profit de l'Institut diplomatique et consulaire du MEAE, 8 cours au sein du Collège européen de sécurité et de défense.

La mutualisation avec l'INHESJ initiée en 2011 s'est poursuivie<sup>3</sup>.

Si le **rapport d'activité de l'IHEDN<sup>4</sup>** 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 types 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).

<sup>1</sup> 3963 journées de formation/auditeurs-participants aux cycles jeunes en 2016, 4478 en 2017, 5038 en 2018 ; 4500 journées de formation/auditeurs-participants aux sessions en région en 2016, 4878 en 2017, 9108 en 2018

<sup>2</sup> 3061 journées en 2017 et 6 280 en 2018

<sup>3</sup> Voir *infra* p. 44.

<sup>4</sup> [https://www.ihedn.fr/sites/default/files/atoms/files/rapport-activite\\_ihedn\\_2018-1.pdf](https://www.ihedn.fr/sites/default/files/atoms/files/rapport-activite_ihedn_2018-1.pdf)

**Le rapport annuel continue à présenter des statistiques par journée et ne met pas en rapport ces éléments « physiques » avec les données comptables.** La mise en œuvre annoncée d'une comptabilité analytique afin de fiabiliser le coût complet d'une session ou d'un auditeur devrait permettre de répondre à l'avenir à cette demande comme permettre d'optimiser la tarification des sessions. Lors de son audition, le Général Destremau a indiqué que la mise en place d'une comptabilité analytique était prioritaire pour assurer un pilotage efficace de l'Institut.

## **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, en exécution, la subvention pour charges de service public a été réduite de 8,8 M€ en 2012 à 7,5 M€ en 2019, soit une baisse de 14,7%. Le budget global est désormais inférieur à 10 M€ (9,7 en 2018) grâce à une part plus importante des recettes propres mais une collecte aléatoire selon les années (2,2 M€ en 2017, 1,8 M€ en 2018).**

En 2018 la part des subventions représente 76% des produits (sensiblement plus qu'en 2017, 72,4%). La part des ressources propres atteint 18,5%, les financements de l'Etat fléchés 4,8% et la taxe d'apprentissage 0,6%. Les charges de personnel représentent 67% des dépenses.

Le montant de la subvention annoncée pour 2019 après régulation est de 7,5 M€. Le nombre d'ETPT autorisé reste de 92. Quatre autres emplois en fonction au sein de l'IHEDN restent rémunérés par d'autres programmes en LFI 2019<sup>1</sup>. 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 des armées 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, mais constitue aussi une contrainte d'organisation qui peut s'avérer coûteuse en cas d'indisponibilité des moyens militaires de transports aériens et de report sur des vols civils au dernier moment. Des efforts de rationalisation ont été engagés pour mutualiser certaines présentations des Armées avec d'autres publics.

**L'équation budgétaire est demeurée sous tension.** Pour autant, et peut-être en raison de l'incertitude sur le niveau de ces recettes soumis au gel pour la subvention et aux aléas pour les ressources propres, l'IHEDN ne parvient pas à consommer ces ressources et dégage régulièrement un excédent (0,17 M€ en CP en 2018 et 0,8 M€ en 2017). **L'entrée dans une phase**

<sup>1</sup> Comme en PLF 2020.

de stabilisation de sa trajectoire financière, en répondant aux exigences de sincérité et de soutenabilité, n'est donc toujours pas acquise.

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

La diminution de la subvention en 2020 alors que l'IHEDN va devoir assurer seul, à partir de second semestre, certaines dépenses mutualisées avec l'INHESJ, voire de reprendre certaines formations dispensées par cette institut sans nécessairement lui transférer les emplois correspondants, et qu'on lui demande, par ailleurs, d'élargir son offre de formation (voir *supra* p.39), risque de maintenir la tension observée en 2018.

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

Compte tenu de la décision du Premier ministre (voir *supra* p.37), l'année 2020 sera le dernier exercice de son activité.

L'INHESI créé en 1989 était pourtant devenu l'opérateur public de référence dans les domaines de la formation et de la recherche liés à la sécurité globale et à la justice, un lieu par lequel la sécurité et la justice se renforcent des échanges avec le monde scientifique grâce à des programmes de recherches de qualité et un lieu de formation pour l'ensemble des acteurs du domaine de la sécurité et de la justice, un lieu de construction de référentiels communs pour des corps amenés à agir ensemble au quotidien dans la lutte contre la criminalité et la délinquance, souvent en tension et avec la tendance simplificatrice à se rejeter la responsabilité du moindre écarts ou de la moindre défaillance.

La décision du Premier ministre oblige désormais à ouvrir une réflexion sur la reprise des formations par les ministères concernés et sur le maintien de l'effort de recherche sans perdre de vue le dialogue entre les institutions la coordination à préserver entre les services concernés des ministères de l'intérieur et de la justice, ainsi que les ressources externes dégagées par ses activités (1,9 M€ en 2018). Il conviendra en outre de maintenir l'Observatoire national de la délinquance et des réponses pénales (ONDRP)<sup>1</sup> en préservant son indépendance par rapport aux deux ministères.

**La commission regrette la suppression de l'INHESJ qui répondait à de véritables besoins. Elle espère que ses deux principaux objectifs, le dialogue entre intérieur et justice et l'effort de recherche scientifique dans ces domaines, ne s'en trouveront pas affaiblis.**

---

<sup>1</sup> 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.

Elle souhaite ici rendre hommage à l'ensemble des collaborateurs qui ont participé à ce travail commun, en soulignant leur dynamisme et la qualité rigoureuse de leur gestion.

## A. MISSIONS ET ACTIVITÉS DE L'INHESJ

### 1. Les missions formalisées dans un plan stratégique

Un nouveau plan stratégique 2018-2021 a donné lieu à l'établissement de feuilles de route d'actions précises et intégrait les objectifs partagés de mutualisation avec l'IHEDN<sup>1</sup>.

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

Afin de traduire et conforter les orientations de ce Plan, un nouveau contrat d'objectifs et de performances entre l'INHESJ et l'Etat a été présenté et signé en même temps que ce dernier. Cette initiative répondait aux observations formulées par la commission dans un précédent rapport<sup>2</sup>.

### 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<sup>3</sup>.

#### a) Les activités de formation

En 2018, l'INHESJ a délivré 112 344 heures/stagiaire de formation (81 196 en 2017) au profit de 2 933 auditeurs et stagiaires (2 201 en 2017)<sup>4</sup> pour 14 043 journées stagiaires (12 030 en 2017) dont 5 494 pour le département formation « sécurité police », 2 357 pour le département « intelligence et sécurité économique » et 6 192 pour le département « risques et crises ».

#### b) Les activités d'études et recherches

Le département « études et recherches » a mené plusieurs travaux de recherche en 2018 s'étalant jusqu'en 2019 sur l'analyse de certains risques et menaces : évolution du financement du trafic de drogue (Narcoter), la violence politique (avec un nouveau volet sur la radicalisation djihadiste des

---

<sup>1</sup> Sénat - [Avis n° 149 Tome IX \(2018-2019\)](#) par MM. Cadic et Mazuir p. 62 et suiv.

<sup>2</sup> Sénat - [Avis n° 142 \(2016-2017\) du 24 novembre 2016, Tome IX](#) - par MM. Bockel et Masseret p. 90.

<sup>3</sup> [https://inhesj.fr/sites/default/files/inhesj\\_files/telechargements/RA\\_INHESJ\\_2018.pdf](https://inhesj.fr/sites/default/files/inhesj_files/telechargements/RA_INHESJ_2018.pdf)

<sup>4</sup> Le nombre d'heures stagiaires qui constitue le critère habituel d'évaluation dans le secteur de la formation pour mesurer l'activité.

femmes en France<sup>1</sup>, la lutte contre le trafic de stupéfiants, l'évaluation des services de sécurité) et participe à des projets de recherche internationaux.

L'institut souhaitait 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 direction chargée des relations publiques et de la prospective a été créée, avec l'ambition d'agrèger 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 des ressources propres**

La réduction d'un cinquième puis la stabilisation du montant de la subvention pour charges de service public depuis 2016 à 6,1 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.

La stagnation des ressources publiques a ainsi pu être compensée par une hausse de 34% des ressources propres, lesquelles atteignent 1,89 M€ en 2018 (1,8 M€ attendus en 2019 et en 2020). Cette augmentation prend en compte la stabilisation de l'activité de formation et une montée en puissance des recettes fléchées en lien avec les travaux de recherche.

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

**Pour 2020, le plafond d'emplois est maintenu au même niveau de 73 ETPT<sup>2</sup> que les années précédentes.** En 2018, le nombre d'ETPT consommés a pu être remonté à 65,77 en 2018.

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 par des recrutements ciblés et moins coûteux (jeunes chercheurs spécialisés, par exemple).

Celle-ci progresse néanmoins 5,16 M€ en 2018 (5,3 M€ prévus en 2019 et en 2020). Cette progression résulte pour une large part du

---

<sup>1</sup> Avec le soutien de l'Unité de coordination de la lutte antiterroriste (UCLAT) et du comité interministériel de prévention de la délinquance et de la radicalisation (CIPRD).

<sup>2</sup> 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.

développement de l'activité et doit être mise en regard de la progression 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. Ce rapprochement des fonctions supports et la concertation sur l'offre de programmes était l'un des axes de leurs plans stratégiques.

**La suppression de l'INHESJ va mettre un terme à ce partenariat et aura deux conséquences auxquelles il faudra remédier :**

- **elle augmentera les coûts de gestion de l'IHEDN**, une part de celle-ci étant mutualisée avec l'INHESJ. Il lui faudra trouver d'autres formes d'adossesment, peut-être avec des structures dépendant du ministère de la défense et présents sur le site de l'École militaire. Les tutelles sur les opérateurs dépendant de ministères et de missions budgétaires différents, ce qui s'était avéré compliqué à mettre en œuvre sous la tutelle du SGDSN risque de l'être plus encore ;

- **la reprise de ces activités par d'autres structures au sein des ministères de la justice et de l'intérieur** avec des synergies à développer avec des structures existantes, ou à l'INSEE s'agissant de l'ONDRP qui doit préserver une forme d'indépendance, voire pour certaines formations à l'IHEDN, **tout en préservant le niveau de ressources propres consolidées par l'INHESJ** au cours des dernières années autour d'un offre des prestations de qualité et clairement identifiées, à hauteur de 1,9 M€ en 2018.

**Globalement, la soutenabilité économique pour le budget de l'Etat de cette opération de simplification reste à démontrer.**

## EXAMEN EN COMMISSION

La Commission a examiné les crédits du programme 129 de la mission « Direction de l'action du Gouvernement, lors de sa réunion du 13 novembre. Après l'exposé des rapporteurs pour avis, un débat s'est engagé entre les commissaires.

**M. Ladislav Poniatowski.** - J'ai bien entendu les chiffres que vous avez cités. Peut-on en savoir plus sur le classement des attaques, sur la nature des attaques et l'importance des dommages ? L'autorité de sûreté nucléaire a une échelle de risque pour classer les incidents intervenus dans les centrales. Dispose-t-on d'un outil équivalent et sinon ne devrait-on pas s'en doter ?

**Mme Hélène Conway-Mouret.** - Je regrette la suppression de l'INHESJ. Cette suppression est incompréhensible. Elle dégageait des recettes, elle formait des personnes venant du public et du privé. Elle a formé 3000 cadres. On crée des structures similaires dans d'autres ministères comme les Affaires étrangères, c'est donc qu'elles sont utiles. L'INHESJ répondait à un besoin, par quoi va-t-il être remplacé ? J'ai l'impression que l'on supprime et que l'on réfléchit ensuite.

**M. Jean-Marie Bockel.** - Je n'arrive pas à comprendre. L'INHESJ est monté en puissance. Il a trouvé sa place. J'avais été impressionné par la qualité de ses travaux et de ses équipements qui permettaient de se former à toutes sortes de situation de crise. Je suis dans un degré total d'incompréhension. Cela m'inquiète pour l'avenir de l'IHEDN.

**Mme Joëlle Garriaud-Maylam.** - Je partage les inquiétudes de nos collègues. Ce n'est hélas pas la première fois qu'on supprime pour recréer, quelques années plus tard, de nouvelles structures ex-nihilo. S'agissant de l'IHEDN, je siège à son conseil d'administration. Je suis inquiète des souhaits de sa tutelle de réduire les orientations internationales de l'IHEDN. C'est une erreur stratégique. Elle est un outil de rayonnement international et d'influence auprès des auditeurs étrangers. Cette dimension doit être absolument maintenue. Il y a aussi des menaces sur le cycle des hautes études européennes de l'ENA. Nos collègues Ronan Le Gleut et Hélène Conway-Mouret, dans leur rapport sur la défense européenne, ont d'ailleurs proposé la création d'une structure comparable à l'IHEDN au niveau européen, cela montre l'utilité de ces structures pour promouvoir la culture et l'esprit de défense et de sécurité.

**M. Olivier Cadic, co-rapporteur pour avis.** - Le tableau ne retrace que les incidents ayant rendu nécessaire l'intervention de l'ANSSI. La très grande majorité des attaques sont prises en compte au niveau des DSI ministérielles. Il fait ressortir des incidents majeurs sur une échelle de 3 (mineurs, notables et majeurs) en fonction des moyens d'expertise et de la durée d'engagement requis pour leur traitement. Nous nous informerons plus avant sur cette échelle de risque.

Souvent les dommages résultent d'une faille non traitée parce que la DSI n'avait pas les ressources humaines disponibles immédiatement comme nous l'avons vu dans la cyberattaque contre l'application Ariane. Petite cause, grand effet. Nous avons constaté que le ministère des finances avait été attaqué cet été sur la plateforme de déclarations de l'impôt sur le revenu. L'ANSSI nous a assuré que la DSI du ministère avait traité cette attaque avec beaucoup de compétences. Il

n'empêche que cela montre la vulnérabilité croissante de nos administrations. Il faut abaisser les coûts de fonctionnement, réduire les effectifs, donc on digitalise, mais fait-on toujours l'effort de sécurité nécessaire ? Avec quel budget ? Combien est mis pour la sécurité dans les nouvelles applications ?

Il sera intéressant de suivre l'évolution de ce tableau dans le temps, car il illustre bien le niveau des menaces. Mais il faudra aller au-delà, de temps à autres, pour apprécier les dommages et voir comment ont été gérés les incidents.

J'ajoute qu'il y a un effort de formation à produire car souvent les responsables « métiers » n'ont pas cet objectif en priorité. Un directeur d'hôpital responsable aujourd'hui doit apprécier les risques de cybersécurité au même niveau que les risques sanitaires dans son établissement. Aujourd'hui, on a besoin de l'informatique pour faire fonctionner un hôpital.

**M. Rachel Mazuir, co-rapporteur pour avis.** - Si Bercy, qui est un des ministères les plus en pointe dans ce domaine, peut être attaqué, quid des ministères moins protégés qui disposent de moins de moyens comme la santé ? D'autant qu'en cette matière, les attaquants ont par construction un avantage sur les défenseurs.

S'agissant de la reprise des activités de l'INHESJ, nous n'avons guère d'informations, si ce n'est que le ministère de la justice et le ministère de l'intérieur disposent de cycles supérieurs de formations susceptibles de reprendre certaines de celles réalisées jusqu'ici par l'INHESJ ; l'IHEDN est en mesure de reprendre les formations sur la cybersécurité et quelques formations dans la sphère de la sécurité, sous réserve que les emplois soient transférés. Pour l'Observatoire national de la délinquance et des réponses pénales, il est envisagé, semble-t-il, son rattachement à l'INSEE. Mais aujourd'hui rien n'est vraiment arrêté, ni pour la formation, ni pour la recherche avec, à la clef, 1,9 M€ de ressources propres à consolider si l'on veut maintenir les activités à l'identique. On peut faire confiance aux deux ministères, mais quid de la coordination et du travail commun qui était un élément important du dispositif actuel.

*Sous le bénéfice de ces observations, lors de sa réunion du 13 novembre 2019, la commission des affaires étrangères, de la défense et des forces armées, pour ce qui concerne le programme 129, a donné, à l'unanimité, 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 2020.*



## LISTE DES PERSONNES AUDITIONNÉES

➤ **Audition en commission plénière :**

- Mercredi 30 septembre 2019

**Mme Claire Landais, secrétaire générale de la défense et de la sécurité nationale et M. Julien Barnu, conseiller pour les affaires numériques.**

*Compte-rendu consultable sur le site Internet du Sénat à l'adresse suivante :*  
<http://www.senat.fr/compte-rendu-commissions/20190930/etr.html#toc3>

➤ **Auditions des rapporteurs :**

- Mardi 17 septembre 2019

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

- Mercredi 6 novembre 2019

**M. le général de corps d'armée Patrick Destremau, directeur de l'Institut des hautes études de défense nationale et de l'enseignement militaire supérieur.**