Projet de loi de finances pour 2026 - Mission « Direction de l'action du Gouvernement » - Programme 129 - Coordination du travail gouvernemental (action 2 Coordination de la sécurité et de la défense, SGDSN, Cyberdéfense) - Examen du rapport pour avis
19 novembre 2025

M. Olivier Cadic, **rapporteur pour avis**. - Le documentaire de France Télévisions que vous venez de voir illustre un vol massif de données de l'Urssaf qui a eu lieu très récemment, et nos concitoyens nous demandent ce que nous faisons pour éviter cela : voilà l'objet du programme 129, que je présente depuis neuf ans. Et nous en sommes toujours là...

Le budget pour 2026 s'inscrit dans le prolongement de 2025, avec une augmentation de 6 %, soit 431 millions d'euros. En réalité, ce montant est inférieur à celui prévu dans le projet de loi de finances pour 2024, qui était de 438 millions d'euros.

Cette revalorisation vise à remplir les objectifs de la revue nationale stratégique 2025 (RNS 2025), laquelle prévoit que l'ambition 2030 « passera par une augmentation des budgets pour accélérer le réarmement de la France et pivoter résolument vers une Nation plus résiliente, prête à faire face à une guerre de haute intensité ».

La part du programme 129 dans cet effort de défense et de sécurité nationale, qui justifie son examen pour avis par la commission, repose sur trois des objectifs stratégiques définis par la RNS 2025 : une résilience cyber de premier rang - j'ai demandé comment mesurer l'évolution de la résilience et j'attends encore la réponse -, une autonomie d'appréciation et une souveraineté décisionnelle garanties, ainsi qu'une capacité à agir dans les champs hybrides. L'atteinte de ces trois objectifs se traduit par un effort budgétaire vers les fonctions de cybersécurité, de protection contre les ingérences numériques étrangères et de soutien aux services de renseignement, selon la répartition suivante pour 2026.

Les crédits du secrétariat général de la défense et de la sécurité nationale (SGDSN) représentent 318 millions d'euros, soit une hausse significative de 23 millions d'euros. Le SGDSN est chargé notamment de l'Agence nationale de la sécurité des systèmes d'information (Anssi), de l'Opérateur des systèmes d'information interministériels classifiés (Osiic) et du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum).

Les moyens du groupement interministériel de contrôle (GIC), qui met en oeuvre les techniques de renseignement au profit des services habilités, sont de 46 millions d'euros, en hausse de 2 millions d'euros. Cette progression s'inscrit dans l'extension des finalités du renseignement aux ingérences étrangères depuis 2024 et à la criminalité organisée depuis la loi visant à sortir la France du piège du narcotrafic.

Sont prévus 67 millions d'euros de fonds spéciaux pour le financement des actions couvertes par le secret de la défense nationale des services de renseignement liés à la sécurité intérieure et extérieure. Cette dotation initiale, essentiellement destinée à la direction générale des services extérieurs (DGSE), demeure stable par rapport à l'exercice 2025, mais elle reste sous-évaluée par rapport à la consommation effective de crédits - plus de 100 millions d'euros -, au regard de la dégradation du contexte sécuritaire et géopolitique.

Voilà pour le volet budgétaire sur la base duquel nous proposerons l'adoption des crédits de la mission.

L'Anssi a dépensé 7 millions d'euros pour renforcer l'accompagnement local aux enjeux de cybersécurité et financer les CSIRT (*Computer Security Incident Response Team*) régionaux. J'avais insisté sur ce point, qui n'était pas prévu dans le budget de l'Agence ; cela montre que les services sont capables de trouver des financements quand la nécessité s'en fait sentir.

Lors de l'audition du SGDSN et de ses chefs de service, j'ai posé des questions qui sont restées sans réponse, ce qui constitue des points d'alerte.

Nous n'avons pas eu de réponse précise sur la publication des stratégies nationales de cybersécurité ou de lutte contre les manipulations de l'information, alors qu'elles avaient été annoncées l'an dernier. Le SGDSN a bien dit que cela dépendait de lui et que les dossiers étaient sur son bureau. Nous attendons donc qu'il veuille bien nous communiquer ces stratégies…

Nous n'avons pas eu plus de réponse sur la recommandation de la Cour des comptes de créer un observatoire public des menaces, qu'elles soient cyber ou informationnelles. Quels sont les retours d'expériences de l'Anssi sur les attaques massives d'institutions telles que France Travail, la DGFiP (direction générale des finances publiques) ou encore l'Urssaf ? Le silence radio de l'Anssi sur les suites à donner est inquiétant. L'Anssi semble se concentrer sur une poignée d'événements de sécurité : dans les statistiques, à peine cinq attaques ont été qualifiées de notables pour toute l'année 2024, alors que les demandes d'assistance du grand public auprès de la plateforme cybermalveillance.gouv.fr, maintenant le 17 cyber, devrait atteindre le demi-million !

Je souhaiterais que l'on puisse faire une mission flash sur le vol massif de données à l'Urssaf, à l'instar du rapport que nous avions rédigé à la suite de la cyberattaque contre la plateforme Ariane du ministère des affaires étrangères. Nous devons montrer que nous réagissons à ce qui s'est passé, en examinant ce que l'Anssi a fait. Pourquoi France Travail est-il attaqué en permanence ? Il n'y a jamais de responsable pour assumer ce qui s'est passé.

Se pose aussi le problème des points d'entrée dans le dispositif de lutte contre les cyberattaques. Mickaël Vallet y reviendra plus en détail, mais, pour ma part, je voudrais savoir sur la base de quels indicateurs et selon quelles justifications seront employés les moyens supplémentaires demandés par l'ANSSI.

Nous allons mettre en oeuvre la directive NIS 2 (*Network and Information Security*), qui vise à élever le niveau de résilience. L'Italie l'a déjà fait : les entreprises ont dû s'enregistrer. Le véritable problème, comme me l'ont dit les Italiens, est de savoir comment mesurer la résilience. En quoi les obligations imposées aux entreprises leur permettent-elles d'être mieux protégées ?

Le retard du projet de loi de transposition des directives relatives à la résilience des entités critiques expose la France à une sanction de 50 millions d'euros. Cela dure depuis plus d'un an ! Cette amende potentielle représente le double de l'augmentation du budget de SGDSN cette année.

D'autres États de l'Union ont transposé plus simplement les directives en appliquant la norme ISO 27000, un système d'assurance qualité. Vendredi dernier, j'ai rencontré le SGDSN du Luxembourg : leur ministère de la défense passe à la norme ISO 27000. Je ne cesse de demander que nos administrations fonctionnent avec un service qualité, ce qui n'est pas le cas jusqu'à présent.

Avec Viginum, nous sommes capables d'aller voir la paille dans l'oeil du voisin. Nous pouvons démontrer comment, grâce à TikTok, un candidat à l'élection présidentielle en Roumanie est passé de 1,5 % à 24 % en quelques semaines. Qui se pose la même question s'agissant d'un candidat du Rassemblement national (RN) dont la notoriété est montée en flèche sur TikTok en quelques semaines au moment des élections européennes ?