…l'avis de la commission sur le projet de loi de finances pour 2026

UN BUDGET 2026 EN HAUSSE FACE AUX CYBERATTAQUES ET MENACES HYBRIDES

Rapport pour avis n° 141 tome IX de MM. Olivier CADIC et Mickaël VALLET sur les crédits de l'action n° 2 « Coordination de la sécurité et de la défense » du programme 129 « Coordination du travail gouvernemental » de la mission « Direction de l'action du Gouvernement ».

Avec **431 millions d'euros pour 2026** au lieu de 406 millions d'euros (M€) votés en loi de finances initiale (LFI) pour 2025, **les crédits de paiement de l'action n°2 « Coordination de la sécurité et de la défense » devraient augmenter de 6 %**.

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*** »[1].

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 (OS) définis par la RNS 2025 que sont une **résilience cyber de premier rang** (OS n°4), une **autonomie d'appréciation et une souveraineté décisionnelle garanties** (OS n°8) et une **capacité à agir dans les champs hybrides** (OS n°9). 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 :

► **318 M€ en crédits de paiement (CP)**, soit une **hausse significative (+23 M€) des crédits du Secrétariat général de la défense et de la sécurité nationale** (SGDSN) qui est en charge notamment de l'agence nationale de sécurité des systèmes d'information (ANSSI), de l'opérateur des systèmes d'information interministériels classifiés (OSSIC) et du service de vigilance et protection contre les ingérences numériques étrangères (Viginum) ;

► **46 M€**, soit une **augmentation de 2 M€** des moyens du **Groupement interministériel de contrôle** (GIC) qui met en œuvre les techniques de renseignement au profit des services habilités (*cf. infra*).

► **67 M€ 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 celle-ci est habituellement abondée en cours de gestion en fonction de l'évolution du contexte sécuritaire et géopolitique.

Quant aux effectifs, **le plafond d'emplois sera revalorisé** de 1 295 équivalents temps plein travaillé (ETPT) en 2025 à 1 337 pour 2026.

[1] Actualisation de la Revue nationale stratégique (RNS 2025) présentée par le Président de la République et publiée le 14 juillet 2025.

1. UNE AUGMENTATION DU BUDGET 2026 EN COHÉRENCE AVEC LES OBJECTIFS FIXÉS PAR LA RNS 2025

A. UNE DOTATION 2025 INSUFFISANTE QUI A NÉCESSITÉ DES ABONDEMENTS EN COURS D'EXERCICE BUDGÉTAIRE

Pour mémoire sur le budget 2025, **la commission avait émis un avis défavorable à l'adoption des crédits de la mission « Direction de l'action du Gouvernement »** au bénéfice d'amendements de crédits déposés ultérieurement en séance en soutien au programme 129, principalement en direction de Viginum ainsi que pour soutenir l'action de l'institut des hautes études de la défense nationale (IHEDN). L'avis de rejet, dont la commission avait précisé qu'il ne devait pas altérer le consensus habituel sur les enjeux de sécurité nationale que représentent la cybersécurité, la lutte contre les ingérences numérique et les fonctions d'appui aux services de renseignement, trouvait son **origine dans la baisse de 3 % initialement proposée par le premier PLF 2025 : 425 M€ y étaient inscrits au lieu des 438 M€ de 2024**.

Les amendements de soutien n'ont pas eu de portée pratique puisque la discussion du premier PLF 2025 n'a pas abouti. **Au final, les crédits de l'action n° 2 « Coordination de la sécurité et de la défense », objet du présent avis budgétaire, ont été ramenés à 406 M€** par la loi de finances pour 2025 promulguée le 14 février 2025.

Cette conjonction entre la reconduction mensuelle par décret des deux premiers mois d'exercice et **les mesures d'économie budgétaire ont nécessité des ajustements** que le SGDSN relata en ces termes lors de son audition du 4 novembre 2025 : « ***Il est très rapidement apparu, dans la gestion de 2025 et dans l'exécution de la loi de finances initiale, que la dotation en crédits de titre 2 était insuffisante pour assurer, sur l'année entière, la rémunération de l'ensemble des agents dans le périmètre du SGDSN*** ». Par ailleurs, l'attribution de nouvelles missions telles que la mise en œuvre de la stratégie nationale de cybersécurité, d'une part, et la lutte contre les manipulations de l'information, d'autre part, allaient également appeler des ajustements en cours d'exercice au bénéfice des priorités opérationnelles :

- s'agissant des dépenses de personnel, une dotation complémentaire de crédits de titre 2 de 5 M€ a été ouverte dans le cadre du schéma de fin de gestion, considérant que le schéma d'emplois pouvait être « légitimement » augmenté de 30 ETP pour minimiser « *les effets délétères sur l'accomplissement des missions opérationnelles du SGDSN* » ;

- s'agissant des missions opérationnelles définies comme prioritaires dans la RNS, qui sont celles de Viginum, de l'Osiic, du GIC et de l'Anssi, un dégel de 18 M€ et une ouverture de 12,4 M€ en CP ont été opérées afin de contribuer, pour partie, au renforcement des programmes interministériels de renseignement technique et d'un certain nombre de programmes classifiés de communication au profit des services de renseignement. Le directeur général de l'Anssi a également précisé que ces abondements avaient également permis de financer des programmes d'infrastructures qui, sans eux, auraient été reportés.

B. UNE DOTATION 2026 QUI MET EN ŒUVRE LES OBJECTIFS D'AUGMENTATION DE MOYENS PRÉVUS PAR LA RNS 2025

Publiée le 14 juillet 2025, la RNS 2025 actualise les travaux menés en 2022 sur l'évolution du contexte stratégique et les moyens adaptés d'y répondre par 11 objectifs stratégiques qui, tous, ont été élaboré sous la coordination du SGDSN. On en retiendra trois qui concourent très directement aux missions des services financés par l'action n° 2 « Coordination de la sécurité et de la défense » et qui sont confortés par la hausse du budget 2026 :

- la revalorisation des moyens du SGDSN est à relier à deux objectifs stratégiques de la RNS 2025 – une résilience cyber de premier rang (OS n°4) et une capacité à agir dans les champs hybrides (OS n°9) – lesquels sont mis en œuvre principalement par l'Anssi pour ce qui concerne la cybersécurité, Viginum pour la lutte contre les manipulations de l'informations et, plus largement pour les menaces hybrides, les services du SGDSN ;

- l'OS n° 8 relatif à l'autonomie d'appréciation et la souveraineté décisionnelle garanties relève de l'action du GIC et de l'utilisation des fonds spéciaux par les services de renseignement.

La RNS 2025 prévoit expressément que « ***l'atteinte de l'ambition 2030 dans le contexte décrit 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*** ». Le fait que **l'augmentation de ces crédits du programme 129 trouve sa légitimité dans l'évolution des dépenses de défense et de sécurité nationale justifie pleinement un avis budgétaire de la commission du Sénat en charge de la défense**.

C. UNE HAUSSE GLOBALE DE 6 % DES MOYENS FINANCIERS ET HUMAINS

Avec 431 M€ pour 2026 au lieu de 406 M€ votés en loi de finances initiale (LFI) pour 2025, les crédits de paiement de l'action n°2 « Coordination de la sécurité et de la défense » augmenteront de 6 %.

L'effort budgétaire vers les fonctions de cybersécurité, de protection contre les ingérences numériques étrangères et de soutien aux services de renseignement, est ainsi réparti pour 2026 :

► 318 M€ en crédits de paiement (CP), soit une hausse significative (+23 M€) des crédits du Secrétariat général de la défense et de la sécurité nationale (SGDSN) qui est en charge notamment de l'agence nationale de sécurité des systèmes d'information (ANSSI), de l'opérateur des systèmes d'information interministériels classifiés (OSSIC) et du service de vigilance et protection contre les ingérences numériques étrangères (Viginum) ;

► 46 M€, soit une augmentation de 2 M€ des moyens du Groupement interministériel de contrôle (GIC) qui met en œuvre les techniques de renseignement au profit des services habilités (cf. infra).

► 67 M€ 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 celle-ci est habituellement abondée en cours de gestion en fonction de l'évolution du contexte sécuritaire et géopolitique, ainsi que l'illustre l'exécution budgétaire de l'exercice 2024 (114,1 M€).

Évolution des crédits du SGDSN par services, des fonds spéciaux et du GIC

(en M€)

<table>
<tr><th></th><th colspan="2">Exécution 2024 en CP</th><th colspan="2">LFI 2025 en CP</th><th colspan="2">PLF 2026 en CP</th></tr>
<tr><th></th><th>Titre 2</th><th>Hors titre 2</th><th>Titre 2</th><th>Hors titre 2</th><th>Titre 2</th><th>Hors titre 2</th></tr>
<tr><td>ANSSI</td><td rowspan="4">90,8</td><td>19,4</td><td rowspan="4">91,2</td><td>26,9</td><td rowspan="4">103,9</td><td>26,9</td></tr>
<tr><td>OSIIC</td><td>25,4</td><td>29,3</td><td>29,3</td></tr>
<tr><td>VIGINUM</td><td>1,8</td><td>2,6</td><td>2,6</td></tr>
<tr><td>SGDSN (autres)</td><td>69,4</td><td>144,7</td><td>154,9</td></tr>
<tr><td>Total SGDSN</td><td colspan="2">206,8</td><td colspan="2">294,9</td><td colspan="2">317,8</td></tr>
<tr><td>Fonds spéciaux</td><td colspan="2">114,1</td><td colspan="2">67,1</td><td colspan="2">67,1</td></tr>
<tr><td>GIC</td><td colspan="2">49,1</td><td colspan="2">44,1</td><td colspan="2">46,1</td></tr>
<tr><td>TOTAL</td><td colspan="2">370,0</td><td colspan="2">406,2</td><td colspan="2">431,1</td></tr>
</table>

Source : réponses au questionnaire budgétaire

Quant aux effectifs, **le plafond d'emplois sera revalorisé** de 1 295 équivalents temps plein travaillé (ETPT) en 2025 à 1 337 pour 2026.

2. SGDSN : PLUS DE MOYENS POUR REMPLIR PLUS DE MISSIONS ET FAIRE FACE À PLUS DE MENACES

La progression du budget 2026 du SGDSN s'explique par l'évolution du contexte international, en particulier le retour de conflits militaires de haute intensité sur le sol européen, ainsi que le changement de paradigme dans les relations entre l'Union européenne et les États-Unis d'Amérique. Cela justifie des investissements supplémentaires dans la politique de défense nationale. L'impact de cette analyse se matérialise par le renforcement significatif des moyens :

- en crédits de personnels (titre 2) avec une progression de 12,7 M€ de la masse salariale par rapport à la LFI 2025 (+13,9 %) ;
- en crédits hors titre 2 (fonctionnement, investissement et intervention), entre la LFI 2025 et le PLF 2026, avec une hausse de 10,2 M€ pour se porter à 213,9 M€ en CP. Cette évolution s'explique par l'augmentation des crédits à destination des capacités techniques interministérielles (CTIM) (+10,4 M€ en CP) et une mesure d'économie sur la subvention de l'IHEDN (-0,5 M€) (cf. encadré ci-après).

Point de situation sur l'IHEDN

À la suite du débat sénatorial sur l'évolution des crédits et missions de l'IHEDN, un contrat d'objectifs et de performance 2026 a été adopté en mars 2025 visant à poursuivre la réforme de l'Institut (baisse de la subvention 2026 à 6,7 M€ contre 7,2 en 2025) tout en consolidant ses effectifs (74 prévus pour 2026 contre 68 en 2025 par un relèvement du nombre d'apprentis) et son offre de services vers les territoires et les jeunes avec une progression du nombre d'auditeurs.

A. 2026 : UNE ANNÉE CHARNIÈRE POUR L'ANSSI

1. Des missions nouvelles : mettre en œuvre la stratégie nationale de cybersécurité et adapter l'agence à la transposition des directives européennes REC et NIS 2

Au titre de la RNS 2025, l'Anssi est chargée de l'application des mesures principales de la stratégie nationale de cybersécurité dont le SGDSN a indiqué en audition à la demande des rapporteurs pour avis qu'une version publique serait publiée dans les prochaines semaines.

Cette stratégie, qui a débuté courant 2025 et porte sur la période 2025-2030, implique l'Anssi dans le pilotage, le suivi et la gouvernance de la cybersécurité de l'État selon trois missions :

- La mission « L'État défend la nation » a pour objectifs la connaissance de la menace et l'élaboration de la réponse de la France aux cyberattaques ; elle est organisée autour de la chaîne du centre de coordination des crises cyber (C4) ;
- La mission « L'État se sécurise » assure le pilotage de la sécurité des systèmes d'information de l'État et des secteurs d'activité d'importance vitale ; elle est organisée autour de la chaîne de sécurité des systèmes d'information de l'État (CINUS , COSINUS , RIM Cyber) ;
- La mission « La Nation se protège » coordonne l'action publique et les efforts privés concourant à renforcer la cybersécurité des particuliers, des entreprises, des associations et des collectivités territoriales. Il est prévu qu'un comité de pilotage des politiques publiques de cybersécurité (C3PC) soit lancé d'ici la fin de l'année 2025.

Ce dernier point rejoint l'autre volet majeur de travail de l'Anssi à conduire des travaux et des consultations auprès des représentants des futures entités assujetties sur le référentiel de sécurité NIS 2 en parallèle de l'examen par le Parlement du projet de loi relatif à la résilience des entités critiques et au renforcement de la cybersécurité, à la suite de l'adoption par le Sénat du texte en première lecture. Parmi les travaux préparatoires à la mise en œuvre de la réglementation sont cités les dispositifs suivants :

- Le lancement de la nouvelle mission « Contrôles et Supervision » début 2025 (5 ETP en juillet 2025) ;

- Des ateliers réguliers avec les associations d'élus locaux pour préparer l'accompagnement des collectivités territoriales ;
- Le développement en cours de finalisation de la plateforme d'enregistrement des futures entités assujetties ;
- Le portail *MesServicesCyber* qui réunit l'offre de services d'accompagnement de l'ANSSI;
- Un travail avec les autres autorités nationales, notamment ACPR et CNIL, de définition des modalités de coopération dans le cadre de la mise en œuvre de la réglementation.

Pour remplir ces nouvelles missions, l'effort budgétaire est essentiellement axé sur le renforcement des ressources humaines. Ainsi **les crédits dits « métiers » resteront stables à 26,9 M€, l'accent portant sur une augmentation du schéma d'emplois qui passera de 656 ETP début 2025 à 668 ETP en 2026**.

Il reste que **la configuration actuelle de l'agence restera à redéfinir en fonction des répercutions de la future loi en cours d'examen à l'Assemble nationale sur le périmètre des entités publiques et privées assujetties**. Force à ce stade est de constater que ni les ministres de tutelle successifs, ni l'Anssi elle-même, n'ont présenté de schéma global sur les contours de ce qui relèvera de la compétence directe de l'agence et de ce qui sera partagé ou confié à d'autres entités institutionnelles – très variées en nombre et en compétences – entre le GIP Acyma Cybermalveillance, les CERT sectoriels (*computer emergency response team*), les CSIRT régionaux (*computer security incident response team*) ainsi que tous les nouveaux opérateurs que l'Anssi aura retenu dans le cadre d'un appel à manifestation d'intérêt pour le renforcement de l'accompagnement local aux enjeux de cybersécurité (AMI-RALEC), doté de quelque 7 millions d'euros sur trois ans.

Les rapporteurs pour avis appellent de leurs vœux une clarification de l'organisation et du financement de l'écosystème de cybersécurité.

À cet égard, la **Cour des comptes** a publié un rapport relatif à « La réponse de l'État aux cybermenaces sur les systèmes d'information civils » dont plusieurs des 11 recommandations rejoignent les sujets de préoccupation des rapporteurs, notamment :

- la nécessité de définir l'articulation entre les CSIRT ministériels, sectoriels et territoriaux et s'assurer de la pérennité de leur financement ;
- la nécessité également de définir une programmation pluriannuelle des moyens de l'ANSSI cohérente avec la stratégie nationale de cybersécurité, le changement d'échelle et l'évolution des missions de l'agence en cohérence avec la loi Résilience et cybersécurité ;

La Cour s'interroge également sur le **modèle économique de fonctionnement du GIP Acyma et du Campus cyber**, ainsi que sur la **simplification des critères de labellisation** des solutions de cybersécurité pour les petites et moyennes entreprises et les collectivités territoriales.

2. Des cyberattaques toujours plus nombreuses

L'année 2024 a notamment été marquée par l'organisation des jeux Olympiques et Paralympiques de Paris (JOP24), l'ANSSI a constaté que la France restait confrontée à une menace particulièrement intense d'attaques informatiques – émanant principalement des États chinois et russe ainsi que de l'écosystème cybercriminel – dont elle a été saisie de **4 386 événements de sécurité**, soit une augmentation de 15% par rapport à l'année 2023.

Sur ce total, l'agence a traité directement 310 événements de sécurité numérique ayant affecté des ministères français. Ces différents événements ont requis un niveau variable d'engagement et d'expertise des agents de l'ANSSI, 304 d'entre eux (dont 221 concernent des compromissions de comptes de messagerie) se sont révélés mineurs au sens où un

engagement minimal a été requis pour leur traitement. Cinq événements peuvent être qualifiés de notables car ils ont requis l'emploi d'expertises particulières pour leur résolution.

Dans le même temps, le ministère des Armées a, quant à lui, traité 115 événements de sécurité cyber (20 incidents et 95 alertes) touchant son périmètre et ayant nécessité une action du COMCYBER (en augmentation de 4 % par rapport à 2023), dont 2 en collaboration avec l'ANSSI et 2 au profit d'établissements publics placés sous la tutelle du ministère des Armées.

Par type de cibles, **310 événements de sécurité numérique ont affecté les ministères** (contre 260 l'année précédente) dont 304 se sont révélés mineurs (*cf. infra* tableau pluriannuel de répartition entre ministères des incidents et leur niveau de gravité).

Tableau de suivi pluriannuel des cyber incidents par ministère traités par l'ANSSI

Ministères	Nombre d'incidents traités par l'ANSSI					Caractérisation des incidents
	2020	2021	2022	2023	2024	
Ministère de l'agriculture et de la souveraineté alimentaire	14	3	2	2	4	
Ministère de l'aménagement du territoire et de la décentralisation	2	2	0	0	3	
Ministère de la culture	11	10	6	16	64	Dont 54 compromissions de messagerie
Ministère des armées	4	5	2	4	14	
Ministère de l'économie, des finances et de la souveraineté industrielle et numérique	18	24	8	25	29	Dont 10 attaques par déni de service (DDoS)
Ministère de l'éducation nationale, de la jeunesse et des sports	58	149	187	160	157	Dont 141 compromissions de messagerie
Ministère de l'enseignement supérieur, de la recherche et de l'innovation	3	0	0	0		
Ministère de l'Europe et des affaires étrangères	14	10	5	8	5	Dont 1 incident majeur
Ministère de l'intérieur et des outre mer*	13	11	4	-	37	
Ministère de la justice	4	4	2	2	6	Dont 4 attaques par déni de service (DDoS)
Ministère de la santé et des préventions	14	6	6	7	7	
Ministère de la transition écologique	18	12	6	5	13	
Ministère du travail, de l'emploi et de l'insertion	6	1	0	5	(voir ministère de la santé)	

Source : réponse au questionnaire budgétaire

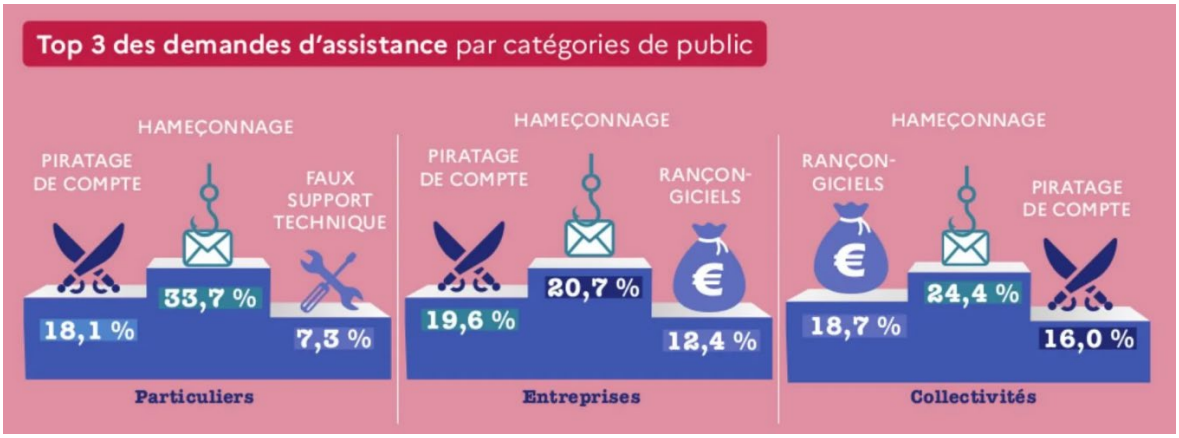
Pour les particuliers, entreprises et collectivités territoriales (hors OIV et OSE[1] suivis par l'ANSSI) le GIP Acyma a enregistré les tendances suivantes pour l'année 2024 :

- la plateforme *Cybermalveillance.gouv.fr* a vu son audience croître de façon significative à **5,4 millions de visiteurs** uniques (+47%) ;

- **420 000 demandes d'assistance ont été enregistrée en 2024** (+49,9 %). **L'hameçonnage demeure la principale menace** avec 1,9 million de consultations d'articles et 64 000 demandes d'assistance, **suivi du piratage de compte ou du rançongiciel** selon que les victimes sont des particuliers, des entreprises ou des collectivités territoriales (cf. schéma ci-après).

[1] Opérateurs d'importance vitale (OIV) et opérateurs de services essentiels (OIV).

Podium des demandes d'assistance sur la plateforme cybermalveillance



(source : GIP Acyma)

Le GIP Acyma explique l'augmentation des statistiques de consultations et de demandes d'assistance par la création de nouveaux services proposés sur le site Cybermalveillance.gouv.fr (e-sensibilisation SensCyber pour le grand public, opération Cactus auprès des collégiens et lycéens, MOOC de gestion de crise cyber SenCy-Crise réalisé en collaboration avec le COMCYBER-MI et la Gendarmerie nationale) et par le lancement du guichet unique 17Cyber lancé en collaboration avec le ministère de l'Intérieur. En année pleine de fonctionnement et de diffusion du dispositif 17Cyber, ces chiffres devraient croître naturellement.

> Il ressort de ces différentes approches de quantification de la cybermenace – **4 386 saisines de l'ANSSI contre 420 000 demandes d'assistance auprès du GIP Acyma** – une **disproportion entre le champ d'action de l'agence et les besoins de l'ensemble de la population qui conforte la nécessité d'une mise en cohérence d'ensemble du dispositif public de réponse aux cybermenaces**.

Ce constat repose la **question récurrente du financement du GIP Acyma** – **dont la subvention** de 845 000 euros accordée par l'Anssi **n'a pas varié depuis 2017** (ce qui équivaut à une réduction tendancielle) – comme des acteurs régionaux qui ont été encouragés à créer des campus cyber et des CSIRT, sans financement pérenne associé.

B. VIGINUM : UNE MISSION RECONNUE EN FRANCE ET À L'INTERNATIONAL

Alors que l'exercice 2025 laissait entrevoir une stagnation des effectifs de Viginum à 53 personnels (42 ETPT), les ajustements en cours d'exercice ont permis au service de poursuivre sa croissance (60 personnels en cours d'année 2025) pour remplir trois nouveaux objectifs visant, premièrement, à **passer d'une posture de défense passive à une posture de défense active**, deuxièmement, à **assumer un rôle de chef de file pour une meilleure défense globale contre les ingérences numériques étrangères**, enfin à **agir sur l'environnement international au profit des intérêts de la France**.

Ces objectifs ont pour objet de mettre en œuvre plusieurs des recommandations émises par le rapport de la **commission d'enquête sur les politiques publiques face aux opérations d'influences étrangères**[1] tendant à la création d'une académie de lutte contre les manipulations de l'information (LMI) et d'un pilotage stratégique contre les ingérences étrangères numériques. Cette montée en puissance de Viginum était également prônée par le rapport d'activité 2023-2024 de la **délégation parlementaire au renseignement (DPR)**[2]. La question de la coordination interministérielle de la stratégie LMI devient cruciale à mesure que

[1] Rapport n° 739 (2023-2024), du 23 juillet 2024, présenté par MM. Dominique de Legge, président, et Rachid Temal, rapporteur.

[2] Rapport n° 211 (2024-2025) relatif à l'activité de la délégation parlementaire au renseignement pour l'année 2023-2024, présenté par M. Cédric Perrin, président.

deviennent opérationnels de nouveaux outils tels que le dispositif « *French Response* » lancé en septembre 2025 par le ministère de l'Europe et des affaires étrangères.

Sur la période du 1er septembre 2024 au 5 août 2025, VIGINUM a diffusé 164 productions à destination de ses partenaires interministériels, parmi lesquelles 128 relevés de détection, 32 notes d'analyse de la menace et 4 notes de caractérisation :

- décembre 2024, le rapport *UN-notorious BIG* de la campagne numérique de manipulation de l'information impliquant des acteurs azerbaïdjanais ciblant les DROM-COM et la Corse ;
- février 2025, le rapport *Guerre en Ukraine : trois années d'opérations informationnelles russes*, synthétisant les principaux modes opératoires informationnels observés depuis le début de la guerre d'agression menée par la Russie en Ukraine ;
- mai 2025, le rapport d'analyse du mode opératoire informationnel russe *Storm-1516* ;
- juin 2025, le rapport sur *African Initiative*, une agence de presse russe, conçue comme l'un des principaux vecteurs d'influence de la Russie en Afrique post-Prigojine, réalisé en collaboration avec le Service européen pour l'action extérieure et le Ministère des Affaires étrangères et du Commonwealth britannique,

La reconnaissance nationale et internationale du service étant établies, il reste à adopter **la stratégie de lutte contre les manipulations de l'information** qui était annoncée pour le courant de l'année 2025.

3. LA REVALORISATION DES FONCTIONS D'APPUI AUX SERVICES DE RENSEIGNEMENT

A. LE GROUPEMENT INTERMINISTÉRIEL ET DE CONTRÔLE

Le Groupement interministériel de contrôle (GIC) met en œuvre des techniques de renseignement (écoutes domestiques et internationales, données numériques, algorithmes de détection des menaces pour la prévention du terroriste) au profit des services de renseignement du premier cercle (DGSI, DGSE, DRSD, DRM, DNRED, TRACFIN), et des services du second cercle qui exercent des missions de renseignement au sein de la police nationale, de la gendarmerie nationale et de l'administration pénitentiaire.

De 44,1 M€ en LFI 2025, le budget du GIC est porté à 46,1 M€ pour 2026.

Cette progression s'inscrit dans le mouvement d'augmentation du nombre des techniques de renseignement utilisées contre la menace terroriste mais aussi contre la criminalité organisée[1] ainsi que l'extension de la technique des algorithmes à de nouvelles finalités en lien avec les ingérences étrangères et la menace cyber autorisées par la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France.

[1] Source : rapport annuel 2024 de la CNCTR

B. LES FONDS SPÉCIAUX : UNE DOTATION À RÉÉVALUER

Le contrôle parlementaire de l'exécution des fonds spéciaux relève de la compétence de la seule commission de vérification des fonds spéciaux (CVFS) en application de l'article 154 de la loi n° 2001-1275 du 28 décembre 2001 de finances pour 2002, le projet annuel de performances se bornant à préciser que les fonds sont principalement destinés à la direction générale de la sécurité extérieure (DGSE)[1].

Comme en LFI 2025, le PLF 2026 prévoit une dotation inférieure aux niveaux de consommation constatés sur les exercices précédents. Les 67,1 M€ en CP pour 2026 sont à rapprocher des quelque 101,2 M€ consommés en 2023 puis 114,1 M€ en 2024.

L'analyse de ces chiffres étant de la seule compétence de la CVFS, vos rapporteurs pour avis se borneront à rappeler la recommandation de celle-ci « *tendant à la présentation d'une estimation de dépense sincère du budget alloué aux fonds spéciaux lors du prochain projet de loi de finances* »[2].

4. LES POINTS DE VIGILANCE DES RAPPORTEURS POUR AVIS

Outre la **clarification de l'organisation et du financement de l'écosystème de cybersécurité** qui est une **recommandation récurrente** – reformulée tous les ans par les rapporteurs pour avis – **plusieurs points de vigilance** sont ressortis de la discussion en commission.

En premier lieu, **des questions restent sans réponse** :

- quant à la publication des stratégies nationales de cybersécurité d'une part, de lutte contre les manipulations de l'information d'autre part ;
- quant au retour d'expérience de l'ANSSI sur les attaques massives d'institutions telles que l'Urssaf, France Travail ou la DGFiP pour ne citer que les plus récentes ;
- quant à la rationalisation des points d'entrée dans le dispositif de lutte contre les cyberattaques ;
- quant au filtre anti-arnaques qui n'a pas encore été mis en œuvre. De ce fait, la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique, dite loi SREN, n'est toujours pas appliquée dans ce domaine ;

En second lieu, **plusieurs constats appellent des ajustements** :

- le Campus Cyber, qui a été créé en 2022, semble être arrivé en fin de cycle d'une mission qui reposait davantage sur la sous-location de surface de bureaux que sur l'animation d'un réseau. L'enjeu de la nouvelle gouvernance du Campus sera de « **transformer la colocation en écosystème** ». Une feuille de route reste donc à tracer en l'ouvrant plus largement aux futures entreprises et collectivités concernées par la directive NIS 2 ;
- la subvention annuelle de 845 000 euros accordée par l'Anssi au GIP Acyma n'a pas varié depuis 2017 : cela équivaut à une réduction tendancielle des moyens ;
- la création d'une académie de lutte contre les manipulations de l'information et d'un pilotage stratégique contre les ingérences étrangères numériques est annoncée dans le cadre de la montée en puissance de Viginum et posera la question de la coordination interministérielle, notamment avec le ministère des affaires étrangères, qui a lancé en septembre 2025 le dispositif *French Response*, pour fournir une riposte en ligne sur les réseaux internationaux lorsque la France est attaquée.

[1] La ventilation qui en est faite entre les différents services de la communauté du renseignement est classifiée.

[2] Source : recommandation n° 1 du rapport précité de la délégation parlementaire au renseignement.

Réunie le mercredi 19 novembre 2025, sous la présidence de M. Cédric Perrin, Président, la commission a émis un avis favorable à l'adoption des crédits de la mission « Direction de l'action du Gouvernement » relative au projet de loi de finances pour 2026.

POUR EN SAVOIR +

Captation vidéo de l'audition de MM. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale, Vincent Strubel, directeur général de l'ANSSI et de Marc-Antoine Brillant, chef du Service Viginum

Cédric Perrin

Président de la commission
Sénateur du Territoire de Belfort
(LR)

Olivier Cadic

Rapporteur
Sénateur représentant les Français établis hors de France
(UC)

Mickaël Vallet

Rapporteur
Sénateur de la Charente-Maritime
(SER)

Commission des affaires étrangères, de la défense et des forces armées
http://www.senat.fr/commission/etr/index.html