N° 141

SÉNAT

SESSION ORDINAIRE DE 2025-2026

Enregistré à la Présidence du Sénat le 24 novembre 2025

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**, *considéré comme rejeté par l'Assemblée nationale, pour* **2026**,

TOME IX

DIRECTION DE L'ACTION DU GOUVERNEMENT

Coordination du travail gouvernemental

(Programme 129)

Par MM. Olivier CADIC et Mickaël VALLET,

Sénateurs

(1) Cette commission est composée de : M. Cédric Perrin, *président ;* MM. Pascal Allizard, Olivier Cadic, Mmes Hélène Conway-Mouret, Catherine Dumas, Michelle Gréaume, MM. André Guiol, Jean-Baptiste Lemoyne, Claude Malhuret, Akli Mellouli, Philippe Paul, Rachid Temal, *vice-présidents ;* M. François Bonneau, Mme Vivette Lopez, MM. Hugues Saury, Jean Marc Vayssouze-Faure, *secrétaires ;* M. Étienne Blanc, Mme Valérie Boyer, MM. François-Noël Buffet, Christian Cambon, Mme Marie-Arlette Carlotti, MM. Alain Cazabonne, Olivier Cigolotti, Édouard Courtial, Jérôme Darras, Mme Nicole Duranton, MM. Philippe Folliot, Guillaume Gontard, Mme Sylvie Goy-Chavent, MM. Jean-Pierre Grand, Ludovic Haye, Loïc Hervé, Alain Houpert, Patrice Joly, Mmes Gisèle Jourda, Mireille Jouve, MM. Alain Joyandet, Roger Karoutchi, Ronan Le Gleut, Didier Marie, Pierre Médevielle, Thierry Meignen, Jean-Jacques Panunzi, Mme Évelyne Perrot, MM. Stéphane Ravier, Jean Luc Ruelle, Bruno Sido, Mickaël Vallet, Robert Wienie Xowie.

Voir les numéros :

Assemblée nationale (**17**ème législ.) : **1906**, **1990**, **1996**, **2006**, **2043**, **2047**, **2048**, **2060**, **2063** et T.A. **180**

Sénat : **138** et **139** à **145** (2025-2026)

SOMMAIRE

Pages

L'ESSENTIEL

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.*

UNE SÉCURISATION DES JEUX OLYMPIQUES DE PARIS 2024

I. 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€)

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

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.

II. 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

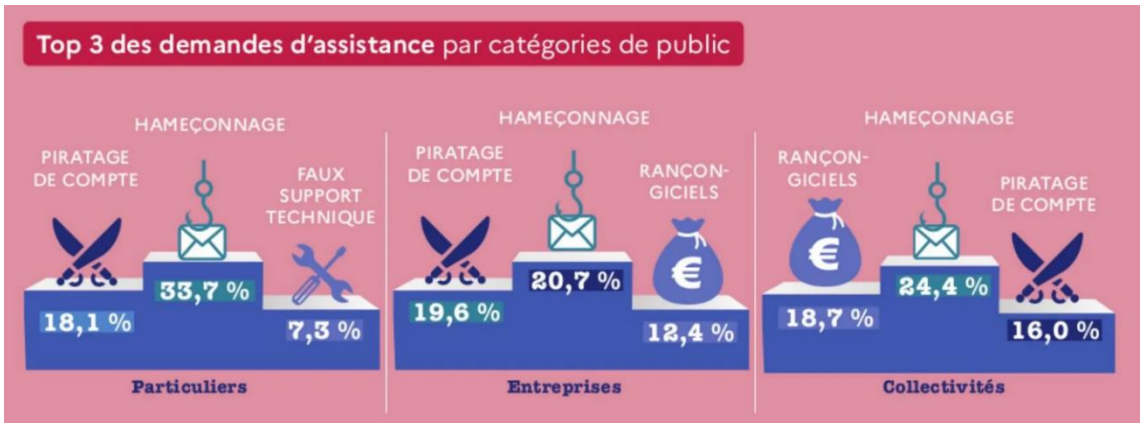
Pour les particuliers, entreprises et collectivités territoriales (hors OIV et OSE[1] suivis par l'ANSSI) le GIP Acyma a enregistré les tendances suivantes pour l'année 2024 :

- 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 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.

---

[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.*

III. 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.

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)[2].

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* »[3].

---

[1] *Source : rapport annuel 2024 de la CNCTR*

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

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

IV. 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.

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.

EXAMEN EN COMMISSION

Au cours de sa réunion du mercredi 19 novembre 2025 la commission des affaires étrangères, de la défense et des forces armées, sous la présidence de M. Cédric Perrin, président, a procédé à l'examen des crédits de la mission « Direction de l'action du Gouvernement » - programme 129 – Coordination du travail gouvernemental.

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 ?

M. Stéphane Ravier. - C'est lunaire !

M. Olivier Cadic, rapporteur pour avis. - La France serait-elle capable d'arrêter une élection si nous étions dans la même situation ? Qui analyse ce qui se passe dans notre pays ?

M. Stéphane Ravier. - Je suis scandalisé par ce qui vient d'être dit ! La démarche du candidat du RN était démocratique. Qu'insinuez-vous ?

M. Cédric Perrin, président. - Mon cher collègue, vous pourrez prendre la parole après les interventions des rapporteurs.

M. Mickaël Vallet, rapporteur pour avis. - Olivier Cadic a présenté le cadre budgétaire et propose d'adopter les crédits pour 2026 - je ne reviendrai pas sur ce point. Je partage un certain nombre de ses interrogations sur la cohérence d'ensemble du dispositif de lutte contre les cyberattaques, mais j'aurai quelques nuances sur l'opposition qui peut être faite entre la notion de guichet unique et le message, certes peu clair de l'Anssi, sur le foisonnement de l'offre de cybersécurité. Je le rejoins néanmoins sur le fait que les missions et les financements de cet écosystème ne sont pas suffisamment clairs.

Je ferai certains constats avant de proposer quelques sujets d'attention.

La configuration actuelle de l'Anssi reste encore largement à redéfinir, ce qui dépendra du périmètre d'application de la directive NIS 2 qui sera adopté dans le cadre du projet de loi relatif à la résilience des infrastructures critiques, actuellement en cours d'examen à l'Assemblée nationale.

À ce stade, ni les ministres de tutelle successifs ni l'Anssi 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, lesquelles sont très variées en nombre et en compétences : le GIP Acyma - cybermalveillance.gouv.fr -, les CERT (*Computer Emergency Response Team*) sectoriels, les CSIRT régionaux, et les nouveaux opérateurs qui sont retenus par l'Anssi dans le cadre de l'appel à manifestation d'intérêt pour le renforcement de l'accompagnement local aux enjeux de cybersécurité, doté de 7 millions d'euros sur trois ans.

Cette nouvelle enveloppe temporaire vient s'ajouter au précédent dispositif de CSIRT régionaux, dont le financement reste à la charge des régions, ce qui n'assure aucune garantie de pérennité. Les financements pourraient s'arrêter du jour au lendemain, par une simple délibération de la région, alors même que l'écosystème global de cybersécurité nous interdit tout trou dans la raquette. La clarification de l'organisation et du financement de cet écosystème est une recommandation que nous reformulons tous les ans.

À cet égard, la Cour des comptes a publié un rapport intitulé *La réponse de l'État aux cybermenaces sur les systèmes d'information civils*. Plusieurs des onze recommandations de ce rapport rejoignent nos sujets de préoccupation : je pense notamment à la nécessité de définir l'articulation entre les CSIRT ministériels, sectoriels et territoriaux et de s'assurer de la pérennité de leur financement, et de prévoir une programmation pluriannuelle des moyens de l'Anssi cohérente avec la stratégie nationale de cybersécurité, laquelle n'est toujours pas publiée.

La réponse qui nous était apportée en audition était assez légère : nous sommes pourtant en droit de connaître le calendrier prévu. Nous sommes également préoccupés par le changement d'échelle et l'évolution des missions de l'Agence, en cohérence avec le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la 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 PME et les collectivités territoriales. Tout le monde ne peut pas en permanence faire appel à l'Anssi. Un organisme de petite taille ou de taille moyenne ou la moindre commune de nos départements doit savoir quels logiciels peuvent être utilisés : une labellisation est nécessaire.

Nous partageons donc un certain nombre de constats. Je reviendrai sur deux d'entre eux : le Campus Cyber et le GIP Acyma.

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.

De nombreuses initiatives, notamment régionales, visaient à se doter de campus cyber. Mais s'il s'agit simplement de mettre dans un même immeuble des entreprises spécialisées sur ce sujet, cela ne produit pas d'émulation ! Même si nos organismes, comme l'Anssi et Viginum, sont reconnus mondialement, on constate que de nombreux pays étrangers ont de meilleurs résultats.

Olivier Cadic a rappelé les différentes approches de quantification de la cybermenace : 4 386 saisines de l'Anssi, contre 420 000 demandes d'assistance auprès du GIP Acyma. Derrière la disproportion entre le champ d'action de l'Agence et les besoins de l'ensemble de la population, se pose la question de la protection du grand public. Les personnes victimes d'une cyberattaque sont démunies : elles cherchent une porte d'entrée. Elles peuvent la trouver avec le GIP Acyma, mais seulement si celui-ci fonctionne correctement, avec les budgets afférents.

Or la subvention 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. Le directeur général de l'Anssi, qui est également le président du GIP, nous a dit de ne pas nous inquiéter pour la pérennité de la plateforme 17 Cyber qu'il considère non comme un point d'entrée unique, mais plutôt comme un « point d'entrée naturel » relié aux autres. Ce n'est pas un jardin à la française, mais cela correspond à la notion de foisonnement de l'offre de cybersécurité. Il reste néanmoins des angles morts, comme le filtre anti-arnaques prévu

par la loi de 2024 visant à sécuriser et à réguler l'espace numérique, dite loi SREN, laquelle n'est toujours pas appliquée dans ce domaine.

Je veux également évoquer la lutte contre les manipulations de l'information, dont la stratégie nationale n'est toujours pas adoptée. Cette stratégie était une demande de notre collègue Rachid Temal, rapporteur de la commission d'enquête sur les politiques publiques face aux opérations d'influences étrangères, qui a rendu ses conclusions en juillet 2024.

Il y a quelques motifs de satisfaction : les ajustements en cours d'exercice ont permis à Viginum de poursuivre sa croissance - 60 personnels en 2025 -, ce qui répond à notre amendement de l'an dernier ; et il est passé d'une posture de défense passive à une posture de défense active, comme l'a montré l'audition par notre commission du chef de ce service le mois dernier.

Il était également question de la création d'une académie de lutte contre les manipulations de l'information et d'un pilotage stratégique contre les ingérences étrangères numériques. Cette montée en puissance de Viginum pose 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.

Là aussi, il reste à structurer une gamme d'outils de détection et de réponse contre les manipulations non seulement de l'information, mais également des élections, avec l'échéance des prochaines municipales. Des entreprises privées françaises ont pris conscience du problème depuis deux ou trois ans ; sans attendre des commandes d'État, elles ont proposé des offres et elles poursuivent actuellement leurs efforts d'innovation.

Au bénéfice de ces observations, nous vous proposons l'adoption des crédits, tout en restant vigilants sur les points d'alerte que nous avons évoqués.

M. Stéphane Ravier. - Monsieur le « petit » rapporteur Cadic, vous avez le droit de ne pas être d'accord avec un adversaire politique, et de faire porter la responsabilité de votre échec électoral sur ses méthodes de communication. Mais faites-le ailleurs qu'en commission ! Ayez le courage d'exprimer vos analyses dans l'hémicycle, pour permettre à vos opposants de s'exprimer tout aussi publiquement.

Nous ne sommes pas réunis en commission pour vous entendre étaler vos états d'âme et nous faire part de votre mélancolie électorale. Contentez-vous de faire ce que vous faites depuis neuf ans, c'est-à-dire de présenter le programme 129, et tout ira pour le mieux !

M. Alain Joyandet. - Sur la sécurité numérique, la question n'est pas de savoir quels moyens doivent être donnés à l'Anssi ou quel retard nous avons en matière de publication de documents ou de transposition de directives.

Depuis quelques dizaines d'années, notre pays et l'Europe ont raté l'entrée dans le monde de la communication. Tant que des milliards de données françaises et européennes, publiques et privées, seront stockées hors de l'Union européenne, nous n'en sortirons pas. Le reste, comme on dit chez moi, c'est un cautère sur une jambe de bois !

La véritable question est donc de savoir si l'Europe, et la France, se saisissent de cet énorme enjeu de sécurité. L'intelligence artificielle se développe à une rapidité exponentielle. Pour rattraper le retard, il faut commencer à agir tout de suite, et le Sénat a son rôle à jouer. Je me souviens que, en 1997, une mission commune d'information de

notre assemblée avait commis un rapport, auquel j'avais participé, sur l'entrée dans la société de l'information. Qu'a-t-on fait depuis ? Rien !

Nous avons regardé l'évolution du phénomène numérique, qui vient des États-Unis, lesquels ont investi des milliards de dollars pour se constituer des entreprises dont la performance est incroyable. L'Europe ferait mieux de s'occuper de ce sujet plutôt que de l'emballage des camemberts ! La France doit, quant à elle, alerter impérativement sur l'importance de cet enjeu stratégique.

Dans notre pays, un certain nombre d'entités publiques et privées ont arrêté d'utiliser Microsoft, et ont mis en place des stratégies « en circuit court » ; des start-up françaises particulièrement performantes proposent des solutions de stockage et des moteurs de recherche très puissants. Il faut développer des solutions en dehors des États-Unis - on ne peut pas toujours accuser les Russes et les Chinois. Le transfert des données dans les tuyaux internationaux rend vulnérables nos millions d'informations qui y circulent. Si nous avions une véritable stratégie européenne, française, nous serions davantage en sécurité.

Quant à l'Agence, elle fait pour le mieux avec les moyens qu'on lui donne, mais, j'y insiste, ce n'est pas vraiment le sujet. Il faut reprendre en main notre sécurité. L'Europe a été capable de faire de grandes choses - je pense à Arianespace -, mais nous ne sommes pas capables d'avoir un *cloud* indépendant des États-Unis.

À l'heure actuelle, ce sont les petites institutions, publiques et privées, qui donnent l'exemple à l'État de ce qu'il faudrait faire. La région Île-de-France, par exemple, cherche des solutions avec des start-up régionales pour accroître son indépendance et sa sécurité. Le recours à ces entreprises augmentera la production française, et donc notre croissance !

M. Cédric Perrin, président. - Nous devons commencer par agir à notre niveau. Pour ma part, j'ai une adresse électronique de La Poste, et pas une boîte Gmail : les données ne sont pas hébergées au même endroit.

M. Olivier Cadic, rapporteur pour avis. - Je souhaite répondre à mon collègue Stéphane Ravier, qui n'a pas tout à fait compris mon propos. J'ai dit que Viginum étudiait les manipulations extérieures et qu'il avait suivi l'élection présidentielle en Roumanie. Je rappelle que cette élection a été arrêtée après le premier tour, ce qui est une décision grave.

Je me demande si la France serait capable d'arrêter une élection présidentielle à l'issue du premier tour si l'on se rendait compte qu'une manipulation étrangère avait favorisé de façon excessive un candidat. Quelques mois avant la Roumanie, il y avait eu à Taïwan une tentative de manipulation du même type, qui avait été détectée et contrecarrée grâce à l'intelligence artificielle.

Viginum ne s'occupe que de la désinformation venant de l'étranger. Aucune analyse n'est faite sur l'évolution de l'explosion de la popularité sur TikTok de certains candidats dans notre pays. Par naïveté peut-être, cette soudaine popularité est associée au charme et au talent du candidat. Je le répète, qui serait capable d'arrêter une élection présidentielle en France si une attaque informationnelle réussie venait changer le cours de notre histoire ? Sommes-nous protégés contre ce risque ? Je dis simplement qu'il s'agit d'un point d'alerte.

Pour répondre à Alain Joyandet, dont je comprends tout à fait la préoccupation, je signale que le *Cloud Act* européen est en cours d'examen. Le *Cloud Cyber Security Scheme* vise à garantir que les données hébergées dans le *cloud* au sein de l'Union européenne restent protégées contre l'accès illégal de pays tiers, notamment en imposant des exigences strictes de souveraineté et de sécurité. Il cherche également à favoriser des fournisseurs européens ou soumis au droit européen pour éviter les risques liés aux lois extraterritoriales étrangères, comme le *Cloud Act* américain.

Mme Hélène Conway-Mouret. - L'ampleur des problématiques mises en évidence par le rapport est considérable, puisqu'il y a à la fois un aspect économique, avec le racket et le vol des données, et un aspect politique, qui, lui, doit nous intéresser fortement.

Vous avez exposé l'ensemble des problèmes auxquels nous devons faire face ; nous devrions nous donner l'ambition de pouvoir y répondre. Le ministère de l'Europe et des affaires étrangères a enfin créé une cellule de riposte, qui emploie quelques dizaines d'agents, quand les services turcs en ont plusieurs milliers, les Russes des dizaines de milliers, et les Chinois encore plus. La création de cette cellule est une bonne chose, mais pourquoi ne pas nous donner dès le départ les moyens de faire mieux ? Pourquoi produire des communiqués de presse une semaine ou quinze jours après un événement, quand tout le monde l'a oublié, au lieu d'utiliser les réseaux sociaux ?

Je suis d'accord avec notre collègue Joyandet. En sous-traitant, nous avons volontairement créé nos propres dépendances vis-à-vis de l'extérieur, qui posent aujourd'hui des questions de souveraineté. Nous avons fait preuve de passivité, on pourrait même dire de lâcheté. Nous aurons beau acheter tous les chars et les avions du monde pour défendre notre pays, nous ne pourrons pas résister à des ingérences étrangères coordonnées à un niveau étatique. Comment faire prendre conscience à nos concitoyens de ces enjeux, notamment dans le cadre des prochaines élections ? La presse a déjà fait état d'attaques coordonnées venant de l'étranger. Qu'attendons-nous donc ?

M. Mickaël Vallet, rapporteur pour avis. - Il est difficile de se comparer avec des pays qui n'ont pas les mêmes standards démocratiques et les mêmes exigences éthiques que les nôtres. Nous ne voulons pas créer des *bots* dans des fermes à trolls pour répondre à de fausses affirmations de manière masquée.

En revanche, avec une cellule de riposte, un nouveau champ d'action s'ouvre. S'il faut toujours des communiqués de presse, des déclarations pesées au trébuchet, des moyens de communication classiques, il faut aussi, pour qu'il n'y ait pas de trou dans la raquette, investir les réseaux sociaux, ces endroits où le message passe par l'ironie et par l'humour, c'est-à-dire en trouvant la bonne tonalité pour démonter une fausse information.

Comme nous l'a expliqué le ministère, cette cellule de l'administration centrale vient en appui aux nouveaux métiers que sont obligés d'investir les chargés de communication ou les porte-parole des ambassades. Ces derniers assurent une vigilance locale, sur des sujets qui concernent la France. Ainsi, en Afrique du Sud il y a quelques semaines, ils ont vu monter une rumeur malveillante, et se sont organisés pour y répondre. Ils parviennent parfois à désamorcer les choses, tout simplement en intervenant sur les réseaux sociaux de manière officielle, mais avec les bons codes. C'est bien à cela que servent les services de riposte.

Ensuite, comment rétablir la vérité en cas de mésinformation massive ? On est là face à une aporie. Continuons-nous à respecter nos libertés publiques ou bien faisons-

nous comme nos adversaires, quitte à être décrédibilisés lorsque nous serons démasqués ? Il est probablement préférable de continuer à respecter nos principes.

J'entends ce qui a été dit sur notre naïveté, sur notre retard par rapport à d'autres grands pays... Je ne suis pas un européiste de la première heure, mais il faut reconnaître que l'échelon européen a fait ce qu'on attend de lui, c'est-à-dire produire de la norme efficace. Je pense au règlement général sur la protection des données (RGPD), qui est repris par d'autres pays, et à la modération des contenus.

Le problème vient de l'équation politique. Que faire quand un pays se comporte de manière impérialiste et promet un retour de bâton, notamment par des mesures tarifaires, si l'on applique nos propres règles ? Les propos que nous entendons aujourd'hui au sein de notre commission sur l'absence de naïveté à avoir vis-à-vis des États-Unis, cela fait bien longtemps que nous aurions dû les entendre ! Car les États-Unis n'ont pas attendu Trump pour se comporter de cette façon. Il faut faire preuve de courage politique.

D'un point de vue technique, les outils existent, mais il faut mesurer ce qu'ils représentent en termes d'investissements. Pour être complètement indépendant, c'est absolument phénoménal ! Il est donc important de distinguer ce qui est important de ce qui ne l'est pas. Une personne cible peut avoir une adresse Gmail, à condition de se contenter de l'utiliser pour faire des commandes sur Amazon, et pas pour échanger des données sensibles.

M. Olivier Cadic, rapporteur pour avis. - À Taïwan, on compare une fausse information à un cancer : il faut y répondre très vite, sinon c'est trop tard. La technique consiste à répondre en 200 mots en deux heures, avec de l'humour, en associant l'administration et des membres de la société civile.

M. Philippe Folliot. - Je voulais aller dans le droit fil du propos d'Alain Joyandet sur la naïveté qui a été assurément la nôtre. Une partie de nos données est hébergée aux États-Unis, mais se pose surtout la question du régime juridique, c'est-à-dire des enjeux relatifs à l'extraterritorialité des lois américaines. Une donnée française adressée à un interlocuteur français qui passe par un tuyau américain, même si cela ne passe jamais physiquement par les États-Unis, peut être récupérée par les autorités américaines. Et l'intelligence artificielle complexifie encore les enjeux.

Ma question sera très technique. Des solutions hybrides sont proposées par un certain nombre d'opérateurs, notamment « Bleu Cloud », de Microsoft, d'Orange et de Capgemini ou S3NS de Google et Thales. Derrière une façade tricolore, ces solutions permettent-elles réellement d'accéder à une souveraineté numérique ? Dans ces conditions, l'Anssi doit-elle accorder sa qualification à ces offres ?

M. Mickaël Vallet, rapporteur pour avis. - Cet exemple est tout à fait pertinent. J'ai interrogé deux fois le Gouvernement sur la question de l'hébergement sur le *cloud* d'Amazon de l'outil prédictif utilisé par EDF pour la gestion des données de maintenance des centrales nucléaires ?

À chaque fois, les réponses ont été assez dilatoires. La première fois, on m'a répondu qu'il s'agissait d'une expérimentation ; la seconde fois, que l'expérimentation avait pris fin, mais qu'aucune donnée sensible n'avait été fournie. Cela montre que de très grandes entreprises peuvent faire preuve de naïveté en considérant qu'Amazon est une bonne solution.

L'Anssi doit-il donner son label ? Nous ne sommes pas des techniciens, mais ce qui est certain, c'est que si l'on garantissait que ces solutions ne tomberont pas sous le coup de l'extraterritorialité du droit américain et qu'il finissait par y avoir un problème, la confiance accordée à la parole de l'Anssi, qui est un élément fondamental dans ce domaine, s'effondrerait. Il faut faire confiance aux techniciens qui ont le sens de l'intérêt national, mais il faut que nous, politiques, puissions fixer comme objectif de ne pas se soumettre à l'extraterritorialité du droit américain.

De ce domaine, on constate tout de même une évolution. Il y a quelques années, le Health Data Hub était utilisé par le ministère de la santé, et un contrat avait été passé entre le ministère de l'éducation nationale et Microsoft. Cela n'est plus tolérable aujourd'hui.

M. Olivier Cadic, rapporteur pour avis. - Le SGDSN a indiqué qu'un cloud sécurisé peut être labellisé SecNumCloud, même s'il n'est pas souverain. L'Anssi considère que la souveraineté est un sujet différent de la cybersécurité.

Quarante-huit heures avant l'invasion de l'Ukraine, les parlementaires de la Rada ont voté à l'unanimité l'autorisation de transfert des données nécessaires au fonctionnement de l'administration en dehors de l'Ukraine. Ces données ont été confiées à Amazon et cela a fonctionné !

M. Pascal Allizard. - Je voudrais revenir sur la problématique du monitoring des élections. Dans le cadre de mes responsabilités à l'AP-OSCE, l'assemblée parlementaire de l'Organisation pour la sécurité et la coopération en Europe, j'ai participé à de très nombreuses missions d'observation électorale. Il faut faire la distinction entre les tentatives d'influencer les électeurs et la manipulation du résultat.

En ce qui concerne la manipulation du résultat, se pose de plus en plus la problématique du vote électronique. Pour prendre un exemple, les dernières élections législatives en Géorgie, il y a un an, ont donné lieu à de nombreuses polémiques, en lien avec l'usage massif du vote électronique. Le gouvernement géorgien sortant avait confié toute la gestion du système de vote électronique à un prestataire américain, ce qui était censé apporter une garantie de qualité.

La mission de court terme observe un process électoral sans entrer dans des commentaires sur les résultats. Nous faisons savoir si nous avons constaté des dysfonctionnements ou des influences extérieures. La mission d'observation est composée généralement de parlementaires de l'AP-OSCE, de l'assemblée parlementaire du Conseil de l'Europe (APCE), de l'Otan, de l'Union européenne et d'observateurs de la société civile. Avec l'évolution des technologies et l'émergence de nouvelles formes d'influence, il est impossible de prétendre que les phénomènes qui ont été évoqués sont inexistants.

Je suis d'accord avec l'analyse d'Olivier Cadic sur la situation française. Parmi les membres fondateurs de la Commission de Venise, la France est pratiquement le seul pays à refuser les missions d'observation. Les États-Unis, la Grande-Bretagne et l'Italie, par exemple, les acceptent. Lors des dernières élections législatives et présidentielles de 2022, les autorités françaises ont mis un veto net et clair à toute observation sur notre territoire. Même si nous sommes de moins en moins naïfs, il est probable que nous soyons confrontés à des compétiteurs privés qui évoluent à une vitesse supérieure à la nôtre.

M. Cédric Perrin, président. - Je remercie les rapporteurs. Je vous invite, mes chers collègues, à être présents en séance pour défendre les crédits de ce programme comme nous l'avions fait l'an dernier sans être malheureusement entendus en CMP.

La commission émet un avis favorable à l'adoption des crédits du programme 129 « Coordination du travail gouvernemental » de la mission « Direction de l'action du Gouvernement ».

LISTE DES PERSONNES ENTENDUES

Mardi 30 septembre 2025 :

- **M. Frédéric Le Bastard**, président de l'InterCERT France et **Mme Haude Costa**, Directrice de l'InterCERT France
- **M. Emmanuel Glimet**, président de section à la 4ème chambre, conseiller maître et **Mme Sylvie Boutereau-Tichet**, conseiller maître à la 4ème chambre, à la Cour des comptes

Mercredi 1er octobre 2025 :

- **Mme Edith Chouteau**, responsable communication Société Wibaie et **MM. David Reverseau et Olivier Luquiau**
- **M. Jérôme Notin**, directeur général du GIP ACYMA Cybermalveillance et **M. Danier Ratier**, Directeur des relations institutionnelles

Mercredi 15 octobre 2025 :

- **M. Emmanuel Lebrun Damiens**, directeur de la communication du ministère de l'Europe et des Affaires étrangères et **Mme Marie-Doha Besancenot**, Conseillère communication stratégique
- **M. Joffrey Célestin-Urbain**, président de Campus Cyber et **Mme Faustine Saunier**

Mardi 4 novembre 2025 :

- **M. Nicolas Roche**, Secrétaire général du SGDSN, **M. Vincent Strubel**, Directeur général de l'ANSSI et **M. Marc-Antoine Brillant**, chef du service Viginum *(audition plénière en commission)*

Mardi 18 novembre 2025 :

- **Général Bruno Courtois** de Sopra Steria