…l'avis de la commission sur le projet de loi de finances pour 2025

CYBERSÉCURITÉ, INGÉRENCES NUMÉRIQUES ET SÉCURITÉ NATIONALE : UN BUDGET 2025 SOUS CONTRAINTE

Rapport pour avis n° 146 tome IX (2024-2025) 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 **425 millions d'euros pour 2025** au lieu de 438 millions d'euros en 2024, les crédits de paiement de l'action n°2 « Coordination de la sécurité et de la défense » subiront une **baisse de 3 %** par rapport à 2024. Seront impactées les fonctions de **cybersécurité**, de protection contre les **ingérences numériques étrangères** et de **soutien aux services de renseignement** qui relèvent de l'activité de défense et de sécurité nationale pilotée par les services du Premier ministre :

► une **baisse de 8 M€ des crédits du Secrétariat général de la défense et de la sécurité nationale** (SGDSN) concerne l'agence nationale de sécurité des systèmes d'information (ANSSI) et le service de vigilance et protection contre les ingérences numériques étrangères (Viginum) ;

► une **réduction de 4 M€ sur les fonds spéciaux** qui assurent le financement de certaines actions des services de renseignement liés à la sécurité intérieure et extérieure (72 M€ pour 2025 au lieu de 76 M€ en 2024)

► une **contraction de 1 M€** des moyens du **Groupement interministériel de contrôle** (GIC) qui met en œuvre les techniques de renseignement au profit des services habilités (*cf. infra*).

Quant aux effectifs, **le plafond d'emplois ne devrait évoluer que marginalement**, passant de 1 283 équivalents temps plein travaillé (ETPT) en 2024 à 1 300 pour 2025.

Les rapporteurs ont salué le fait qu'en dépit de l'augmentation dès 2023 des menaces de tous ordres (cyberattaques, guerre informationnelle, opérations de déstabilisation des outre-mer, tensions causées par les conflits en Ukraine et au Moyen-Orient, etc.) **les services et opérateurs du programme 129 ont préparé et protégé avec succès les grands rendez-vous de l'année 2024** : les élections européennes puis législatives et notamment les Jeux olympiques et paralympiques (JOP 2024).

Ce budget 2025 implique des ajustements et une redéfinition des missions, notamment de l'ANSSI, dont l'année 2025 devait correspondre à un changement d'échelle nécessaire à la transposition de la directive dite « NIS 2 », et de Viginum qui devait poursuivre la montée en puissance de ses services opérationnels et de ses partenariats internationaux.

Le rapport identifie les contraintes causées par ce budget et signale le risque d'aggravation de 25 M€ de la baisse des crédits de ce programme annoncé par un amendement du Gouvernement déposé lors de la discussion du texte à l'Assemblée nationale.

En conséquence, le mercredi 20 novembre 2024, sous la présidence de M. Cédric Perrin, Président, au terme d'un large débat[1], la commission a émis un avis défavorable à l'adoption des crédits de la mission « Direction de l'action du Gouvernement » relative au projet de loi de finances pour 2025, au bénéfice d'amendements de crédits déposés ultérieurement en soutien au programme 129.

[1] Compte rendu de la réunion de commission du 20 novembre 2024.

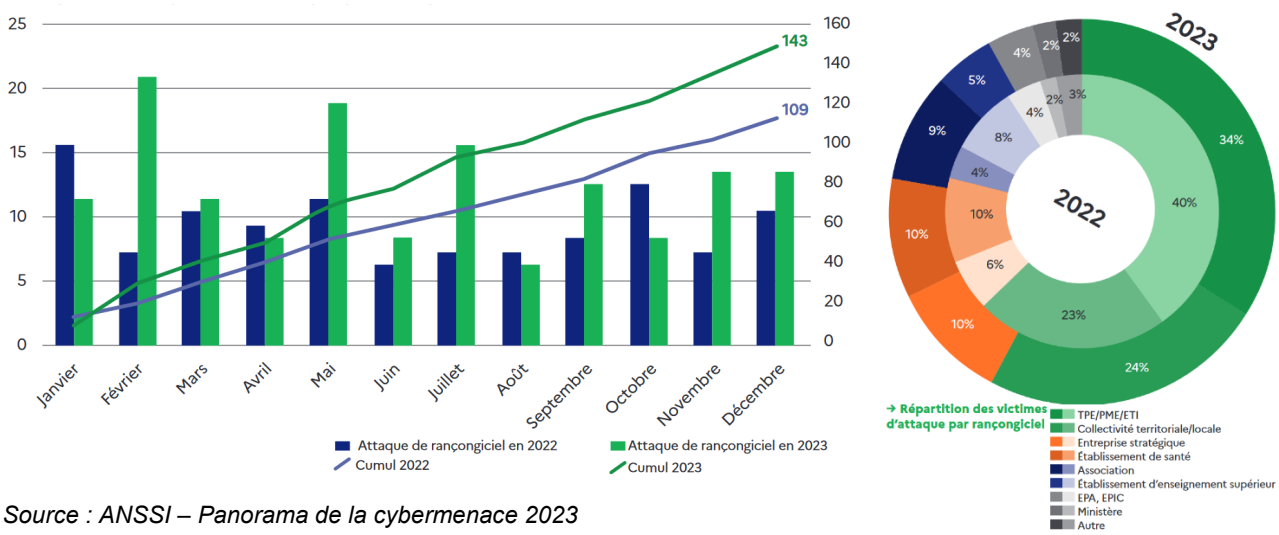
1. UNE AUGMENTATION DU NIVEAU DE LA CYBERMENACE EN 2023 AVEC COMME PRIORITÉ LA SÉCURISATION DES JEUX OLYMPIQUES DE PARIS 2024

A. DES CYBERATTAQUES PLUS NOMBREUSES ET PLUS DIVERSIFIÉES

L'ANSSI publie chaque année un panorama de la cybermenace, lequel présente pour l'année écoulée une **augmentation du niveau de la cybermenace**. En 2023, **3 703 événements de sécurité**, contre 3 018 en 2022, ont été portés à la connaissance de l'ANSSI dont **1 112 incidents traités** par l'agence contre 832 en 2022. Les cyberattaques sont reliées à **trois sources principales** : la **Chine**, la **Russie** et l'**écosystème cybercriminel**.

Les attaques par rançongiciels portées à la connaissance de l'agence ont connu une progression de 30 % passant de 109 en 2022 à 143 en 2023, ces nombres non exhaustifs se limitent aux cas nécessitant une analyse de l'agence mais traduisent une tendance générale qui n'épargne aucun secteur d'activité avec par ordre de ciblage les TPE/PME/ETI (34 %), les collectivités territoriales (24 %), les établissements de santé (10 %) et les entreprises stratégiques (10 %).

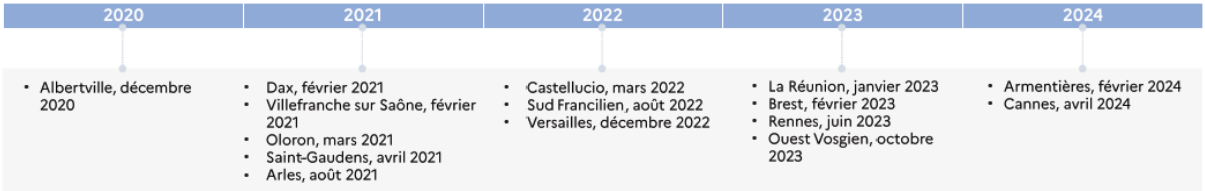
Évolution et répartition des attaques par rançongiciels



Source : ANSSI – Panorama de la cybermenace 2023

Concernant le secteur de la santé, 30 établissements ont été affectés par des compromissions et chiffrements causés par des rançongiciels en 2022 et en 2023. Durant cette période, le secteur de la santé a représenté à lui seul 10 % des incidents liés à des rançongiciels signalés à l'ANSSI.

Exemples d'attaques par rançongiciel ayant touché des centres hospitaliers en France



Source : ANSSI (Secteur de la santé – État de la menace informatique – octobre 2024)

Le niveau de maturité des universités et des hôpitaux en matière de cybersécurité demeure très bas. L'AP-HP qui fait figure d'exception grâce à la masse critique que son budget numérique et cyber permet pour développer de bonnes pratiques, notamment celle de **consacrer 10 % du budget numérique à la cybersécurité**.

Par type de cibles, **260 événements de sécurité numérique ont affecté les ministères** (contre 227 l'année précédente) dont 246 se sont révélés mineurs (*cf. infra* tableau pluriannuel de répartition entre ministères des incidents et leur niveau de gravité).

Tableau 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	
Ministère de l'agriculture et de l'alimentation	14	3	2	2	
Ministère de la cohésion des territoires	2	2	0	0	
Ministère de la culture	11	10	6	16	Dont 8 compromissions de compte de messagerie
Ministère des armées	4	5	2	4	
Ministère de l'économie des finances et de la relance	18	24	8	25	Dont 13 attaques par DDoS (déni de service)
Ministère de l'éducation nationale, de la jeunesse et des sports	58	149	187	160	Dont 181 compromissions de comptes 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	Dont 1 opération de cyberdéfense
Ministère de l'intérieur *et des outre mer**	13	11	4		
Ministère de la justice	4	4	2	2	
Ministère de la santé et des préventions	14	6	6	7	
Ministère de la transition écologique	18	12	6	5	
Ministère du travail, de l'emploi et de l'insertion	6	1	0	5	

Source : réponse au questionnaire budgétaire

Le panel d'attaques reste très disparate allant des compromissions de comptes de messagerie à des attaques par déni de service pour les moins graves. Une quinzaine d'attaques notables ou significatives ont requis l'intervention à moyen et long terme d'expert de l'ANSSI.

Pour les particuliers, entreprises et collectivités territoriales (hors OIV et OSE[1] suivis par l'ANSSI) :

- En 2023, 3,7 millions de visiteurs ont consulté la plateforme *Cybermalveillance.gouv.fr*, dont la fréquentation se stabilise.
- En parallèle 280 000 demandes d'assistance ont été enregistrées via l'outil de diagnostic en ligne, avec une augmentation de +13 % pour les particuliers et +17 % de la part des collectivités.

B. JEUX OLYMPIQUES DE PARIS 2024 : MISSION ACCOMPLIE

S'agissant du panorama des menaces, les chiffres donnés par l'ANSSI peuvent paraître modestes mais ils ne sont pas contradictoires avec le niveau élevé d'attaques. Ainsi, si « seulement » 548 tentatives d'attaques, dont 83 ont produit des effets, ont été dénombrées par l'ANSSI sur les JO de Paris, c'est sur la base d'une analyse des 55 milliards d'attaques individuelles répertoriées par ATOS (opérateur officiel du comité international olympique en charge du consortium numérique et cyber) contre moins de 5 milliards aux JO de Tokyo en 2021. Le niveau de traitement des données est donc sans précédent, sachant qu'un seul événement au sens de l'ANSSI peut recouvrir une multitude d'attaques individuelles. C'est notamment le cas des attaques par saturation des réseaux.

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

Il est ici important de rappeler que la menace n'a pas été surévaluée au regard de l'absence d'indicent grave, mais que la menace a bien été évaluée, les attaques ont bien eu lieu et le niveau de défense a été efficace.

Bilan du 8 mai au 8 septembre 2024

Menace cyber

548 événements de cybersécurité affectant des entités en lien avec l'organisation des JO ont donné lieu à un traitement par l'ANSSI

- dont 465 signalements (impact bas pour les systèmes d'information) ;
- et 83 incidents (actions malveillantes ayant atteint le système d'information de la victime).

Menace de la manipulation de l'information

Sur la période Viginum a identifié 43 manœuvres informationnelles ayant ciblé les Jeux. En outre deux campagne numériques planifiées et coordonnées ont impliqué des acteurs pro-azerbaïdjanais. Au demeurant, les trois principaux axes narratifs hostiles n'ont pas remis en cause l'organisation des JO, ni trouvé de relais significatif :

- le récit selon lequel la France était incapable d'accueillir les JO 2024 dans de bonnes conditions ;
- l'instrumentalisation du niveau réel de la menace terroriste pesant sur les JO 2024 ;
- le ciblage et le dénigrement des instances d'organisation de l'événement.

Il faut aussi rappeler qu'en plus des 12 millions d'euros consacrés spécifiquement par l'ANSSI, l'agence a en outre sacrifié 30 % de ses capacités à la sécurisation des Jeux, par des activités d'audit et d'accompagnement. Par ailleurs 100 % de ses équipes ont été mobilisées pendant l'événement, nécessitant la formation d'agents non spécialistes à la gestion des notifications d'alertes cyber. Il faut plus largement saluer la mobilisation de l'ensemble des services du SGDSN.

2. LE BUDGET 2025 DU SGDSN : BAISSE DES CRÉDITS ET STAGNATION DES RESSOURCES HUMAINES

Avec 425 millions d'euros au lieu de 438 millions d'euros, les crédits de paiement de l'action n°2 « Coordination de la sécurité et de la défense » subiront en 2025 une baisse de 3 % par rapport à 2024. **Sont donc impactés dans ce périmètre budgétaire le cœur de l'activité de défense et de sécurité nationale** à savoir **les fonds spéciaux** qui financent certaines actions des services de renseignement liés à la sécurité intérieure et extérieure (72 millions d'euros en 2025 au lieu de 76 millions d'euros en 2024) et le **Groupement interministériel de contrôle** (GIC) qui centralise les techniques de renseignement (*cf. infra*).

Les 3 services du SGDSN en charge de la cybersécurité et de la lutte contre les manipulations de l'information (ANSSI, OSIIC et Viginum) vont devoir fonctionner avec 8 millions d'euros en moins. Les réductions de crédits hors titre 2 sont précisément détaillées dans le tableau ci-dessous. En revanche, la ventilation entre services des dépenses de personnel (titre 2), qui subissent une réduction d'un million d'€ n'est pas présentée. Cela reflète un **manque global de lisibilité dans le projet annuel de performance de la répartition des crédits de personnels ou de la projection pluriannuelle des crédits**.

Évolution des crédits du SGDSN par services

	Exécution 2023 en CP		LFI 2024 en CP		PLF 2025 en CP	
	Titre 2	Hors titre 2	Titre 2	Hors titre 2	Titre 2	Hors titre 2
ANSSI	78 897 037	26 433 395	92 509 724	30 727 870	91 569 378	27 234 359
OSIIC		32 892 606		33 574 212		31 381 774
VIGINUM		1 818 714		2 365 186		2 500 000
Total SGDSN	190 950 534		223 320 925		215 989 301	

Source : réponses au questionnaire budgétaire

Quant aux effectifs, le plafond d'emplois ne devrait évoluer que marginalement, passant de 1 283 équivalents temps plein travaillé (ETPT) en 2024 à 1 300 pour 2025.

Évolution des effectifs du SGDSN par services

	Effectifs 2023		LFI 2024		PLF 2025	
	ETP (Schéma d'emplois)	ETPT (plafond d'emplois)	ETP (Schéma d'emplois)	ETPT (plafond d'emplois)	ETP (Schéma d'emplois)	ETPT (plafond d'emplois)
Viginum	0	898,2	0	42	0	42
OSIIC	+9		+10	135	0	138
ANSSI	+41,7		+40	644	0	657
SGDSN hors Viginum, OSIIC et ANSSI	+12,7		0	189	0	187
Total SGDSN hors GIC	**+63,4**	**898,2**	**+50**	**1 010**	**0**	**1 024**
GIC	+34	210,4	+6	273	0	276
Total BOP SGDSN	**+97,4**	**1 108,6**	**+56**	**1 283**	**0**	**1 300**

Source : réponses au questionnaire budgétaire

A. LES CONTRAINTES DU BUDGET 2025 SUR LES FONCTIONS DE CYBERSÉCURITÉ ET DE LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION

1. L'ANSSI : des adaptations à envisager pour supporter la charge des nouvelles missions en 2025

L'ANSSI avait demandé un budget de 35 millions d'euros et 60 emplois supplémentaires notamment pour conduire la réforme nécessaire pour appliquer le projet de loi relatif à la résilience des entités critiques et au renforcement de la cybersécurité, dont fait partie la transposition de la directive dite NIS2 (*Network and Information Security*) ; **l'agence n'aura que 27 millions d'euros (hors T2) et aucun poste en plus**.

L'objectif majeur de l'agence pour 2025 reste de réussir la transformation de l'ANSSI en vue de la transposition de la directive NIS 2. Celle-ci prévoit un accroissement du périmètre de compétence de l'agence de quelque 500 OIV à environ 15 000 entreprises dont le suivi constitue un changement d'échelle pour l'agence et nécessite une reconfiguration de son offre de services.

Cette contrainte budgétaire annonce nécessairement des ajustements sur plusieurs postes.

- la préparation de la transposition de la directive NIS 2 : le passage à l'échelle qui était annoncé au sein du dernier rapport devra être retardé ;
- le maintien de son expertise de pointe : la création d'un laboratoire dédié à l'intelligence artificielle devra être retardée ;
- la création d'un second centre de données sécurisées devra être reportée ;
- l'agence ne pourra pas non plus continuer à étendre sa couverture des ministères, ni faire l'acquisition de nouveaux téléphones sécurisés.

2. Viginum : un coût d'arrêt au développement de la lutte contre les manipulations de l'information

En matière de lutte contre les manipulations de l'information (LMI), le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) a été créé à l'automne 2021 afin de détecter et de caractériser les ingérences numériques étrangères (INE).

Le rapport de la commission d'enquête sur les politiques publiques face aux opérations d'influences étrangères[1] a souligné le rôle central qu'occupe ce service en France et en Europe après seulement 2 ans de mise en œuvre d'une politique de publication de rapports sur des opérations de déstabilisation à grande échelle. Le bilan quantitatif pour 2023 s'établit à 236 notes (détection de phénomènes inauthentiques, d'INE et d'analyse de la menace) avec une accélération en 2024 (158 notes sur le 1er semestre). Dans le même temps, quatre rapports publics ont dénoncé des opérations attribuées à des acteurs pro-russe ou pro-azerbaïdjanais (RRN, Portal Kombat, Nouvelle Calédonie, Matriochka).

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

Il faut signaler que **pour la première fois depuis sa création en 2021, les effectifs de VIGINUM ne vont pas augmenter**. Une telle **stagnation** nous paraît **inquiétante alors que les manipulations de l'information continuent de croître quantitativement et qualitativement** du fait également de **l'intelligence artificielle**. Viginum devait passer de 42 à 65 ETPT fin 2025, il restera à 42, pour environ 53 personnels fin 2024 (au lieu de 59), ce qui ne permettra pas de développer les programmes de coopérations européenne et internationale et le projet de développement d'une académie de la LMI portée par une recommandation de la commission d'enquête. Le déficit de 12 postes en 2025 par rapport à la progression initialement prévue représente une économie d'environ 1 million d'€, mais aussi un **risque de limitation capacitaire** pour les équipes opérationnelles alors même que l'année 2025 doit être celle du lancement d'une stratégie nationale de lutte contre les manipulations de l'information.

B. UNE SOUS-BUDGÉTISATION DES FONCTIONS D'APPUI AUX SERVICES DE RENSEIGNEMENT

1. Les fonds spéciaux : une sous-budgétisation récurrente

Les fonds spéciaux ont pour objet de financer les opérations des services de renseignement qui doivent demeurer couvertes par le secret de la défense nationale afin d'assurer la sécurité extérieure et intérieure de la Nation. Le contrôle parlementaire de l'exécution de ces dépenses 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].

En revanche, le montant voté en loi de finances initiale ainsi que l'exécution budgétaire globale des crédits sont des données publiques figurant dans les annexes aux documents budgétaires. Celles-ci font apparaître de manière récurrente une sous-budgétisation systématique, le montant de 76 M€ étant invariablement voté depuis 2021, indépendamment du niveau d'exécution, systématiquement supérieur de près de 30 % en 2022 et 2023 (cf. tableau ci-dessous)

Évolution de la dotation et de l'exécution des crédits de fonds spéciaux

2022		2023		2024		2025	
LFI	Exécution	LFI	Exécution	LFI	Exécution	PLF	Exécution
75 976 462	101 259 770	75 976 462	102 126 462	75 976 462	/	71 924 802	/

Source : réponses au questionnaire budgétaire et annexes aux projets de lois de règlement de 2022 et 2023

Aussi, la réduction de 4 M€ sur les fonds spéciaux (72 M€ pour 2025 au lieu de 76 M€ en 2024) conduit à réitérer la **recommandation tendant à allouer une enveloppe de crédits conforme au principe de sincérité de la prévision budgétaire**.

2. Le groupement interministériel et de contrôle : baisse de crédits et hausse d'activité

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. Le budget 2025 opère une réduction de 1 M€.

Évolution des crédits du GIC

	Exécution 2023 en CP		LFI 2024 en CP		PLF 2025 en CP	
	Titre 2	Hors titre 2	Titre 2	Hors titre 2	Titre 2	Hors titre 2
GIC	16 313 366	26 381 022	18 063 097	29 017 585	18 933 443	27 078 676
Total	42 694 388		47 080 682		46 012 119	

Source : réponses au questionnaire budgétaire

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

Cette contraction de moyens s'inscrit **à rebours des besoins du GIC pour 2025** :

- le nombre des techniques de renseignement utilisées ont augmenté en 2023, avec 94 902 demandes des services soit +6 % par rapport à l'année 2022 et +29,1 % par rapport à 2019, première année du suivi statistique ; 24 209 personnes ont été surveillées par ces techniques (+15 % par rapport à 2022 et +9 % par rapport à 2019). Cette augmentation est selon la commission nationale de contrôle des techniques de renseignement (CNCTR) à mettre en lien avec l'évolution de la menace terroriste mais aussi de la criminalité organisée[1] ;

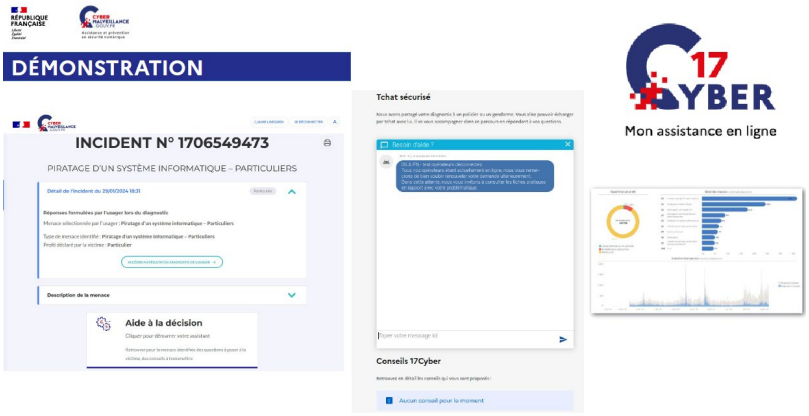
- par ailleurs, la loi 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France a étendu la possibilité d'appliquer la technique des algorithmes à deux nouvelles finalités en lien avec les ingérences étrangères et la menace cyber. Or le développement de ces techniques nécessite des moyens techniques et humains importants pour en assurer le développement et l'exploitation sur des volumes importants de données (*big data*).

C. LES OPÉRATEURS : UNE GOUVERNANCE ET DES MISSIONS À CLARIFIER

1. GIP ACYMA cybermalveillance : un acteur efficace en dépit d'une gouvernance à clarifier

Deux projets emblématiques de la cybersécurité – le filtre anti-arnaque et la plateforme 17Cyber – ont motivé la visite du siège du GIP Acyma pour comprendre les raisons des retards pris sur des dispositifs initialement destinés à entrer en fonction avant les JOP 2024.

Cybermalveillance et 17 Cyber



Démonstration de la nouvelle plateforme 17 Cyber
Source : GIP Acyma

Visite du siège du GIP Acyma

Deux constats peuvent être faits, qui ne relèvent pas du GIP Acyma :

- La mise en place d'un **filtre anti-anarques** a été autorisée par la loi dite « SREN »[2]. Alors que ce filtre devait être fonctionnel pour les JOP, l'appel d'offres lancé par la direction générale des entreprises (Bercy) concernant le développement et la gestion du filtre est toujours en cours. Le GIP ACYMA a été écarté de l'appel d'offres alors qu'il était le candidat idéal en termes de compétence et d'outil et qu'il existe un risque que le marché soit remporté par un acteur privé étranger. Pour l'heure, **ce service n'est donc toujours pas mis en œuvre**.

- Nous pouvons également regretter que la **plateforme 17Cyber** n'ait pas été lancée en temps voulu alors qu'elle est opérationnelle depuis le mois mars 2024, dans les délais et les coûts initialement prévus. Alors qu'il s'agissait d'une priorité annoncée pour contribuer à la sécurisation des JOP, la plateforme n'avait pas été inaugurée par le ministre de l'Intérieur qui assure la tutelle de ce dispositif, en raison des événements intervenus en Nouvelle-Calédonie. Puis en juin, la dissolution est intervenue, laissant en suspens le lancement de cette

[1] Source : rapport annuel 2024 de la CNCTR

[2] Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique

plateforme. Surtout, Il y a toujours urgence à lancer une campagne de diffusion de ce nouvel outil auprès du grand public. La démonstration s'est avérée pleinement opérationnelle et il convenait donc de le signaler au ministre de l'intérieur actuel pour qu'il assure le portage[1].

Ces constats appellent une **meilleure coordination de la gouvernance entre le SGDSN et les différents ministères de tutelle de l'opérateur**.

2. L'IHEDN : les réductions d'effectifs envisagées nécessitent une clarification des missions et objectifs

L'Institut des hautes études de défense nationale (IHEDN) est un établissement public national, placé sous la tutelle du Premier ministre, ayant pour mission de développer l'esprit de défense, de participer au renforcement de la cohésion nationale, de sensibiliser aux questions internationales et de contribuer au développement d'une réflexion stratégique portant sur les enjeux de défense et de sécurité. Depuis 2010, ses effectifs ont été réduits, passant de 111 à 86 en 2024, dont 15 mises à disposition, soit 71 ETP (- 22,5 % depuis 2012).

Serait envisagée pour 2025 une réduction de 5 emplois, première étape d'un rabot total de 17 emplois sur trois ans, soit près de 24 % des effectifs actuels. Ne subsisteraient que 54 ETP dans 3 ans. Ce n'est pas tant la baisse des moyens sur 2025 que l'engrenage triennal que cela risque d'engendrer sur le maintien des missions de l'institut, lequel a accru ses activités de formation et d'information avec plus de 2 500 auditeurs, dont 600 étrangers dans le cadre d'une session nationale, de 6 sessions en région dont une en outre-mer, de 8 cycles jeunes dont un en outre-mer, de sessions européennes et internationales, de cycles d'intelligence économique, etc.

Une telle trajectoire conduirait nécessairement l'institut à reconsidérer ses missions et ses objectifs, alors même que **la fonction stratégique d'influence de l'IHEDN s'inscrit dans les priorités de la revue nationale stratégique de 2022, au même titre que l'ANSSI participe à la cyberdéfense et Viginum à la guerre contre la désinformation**.

POUR EN SAVOIR +

- **Captation vidéo de l'audition de MM. Stéphane Bouillon, 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**
- **Compte rendu de la réunion de commission du 20 novembre 2024**

Commission des affaires étrangères, de la défense et des forces armées

http://www.senat.fr/commission/etr/index.html

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)

[1] Au final, le lancement opérationnel de la plateforme 17Cyber s'est déroulé le 17 décembre 2024 en présence du directeur général de l'ANSSI et des directeurs généraux de la Police nationale et de la Gendarmerie nationale.