N° 146

SÉNAT

SESSION ORDINAIRE DE 2024-2025

Enregistré à la Présidence du Sénat le 21 novembre 2024

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* **2025**,

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. Joël Guerriau, Jean-Baptiste Lemoyne, Akli Mellouli, Philippe Paul, Rachid Temal, *vice-présidents ;* M. François Bonneau, Mme Vivette Lopez, MM. Hugues Saury, Jean-Marc Vayssouze-Faure, *secrétaires ;* MM. Étienne Blanc, Gilbert Bouchet, Mme Valérie Boyer, M. 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, André Guiol, Ludovic Haye, Loïc Hervé, Alain Houpert, Patrice Joly, Mmes Gisèle Jourda, Mireille Jouve, MM. Alain Joyandet, Roger Karoutchi, Ronan Le Gleut, Claude Malhuret, Didier Marie, 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.) : **324**, **459**, **462**, **468**, **471**, **472**, **486**, **524**, **527, 540** et T.A. **8**

Sénat : **143** et **144** à **150** (2024-2025)

SOMMAIRE

Pages

L'ESSENTIEL

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 débat1, **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.*

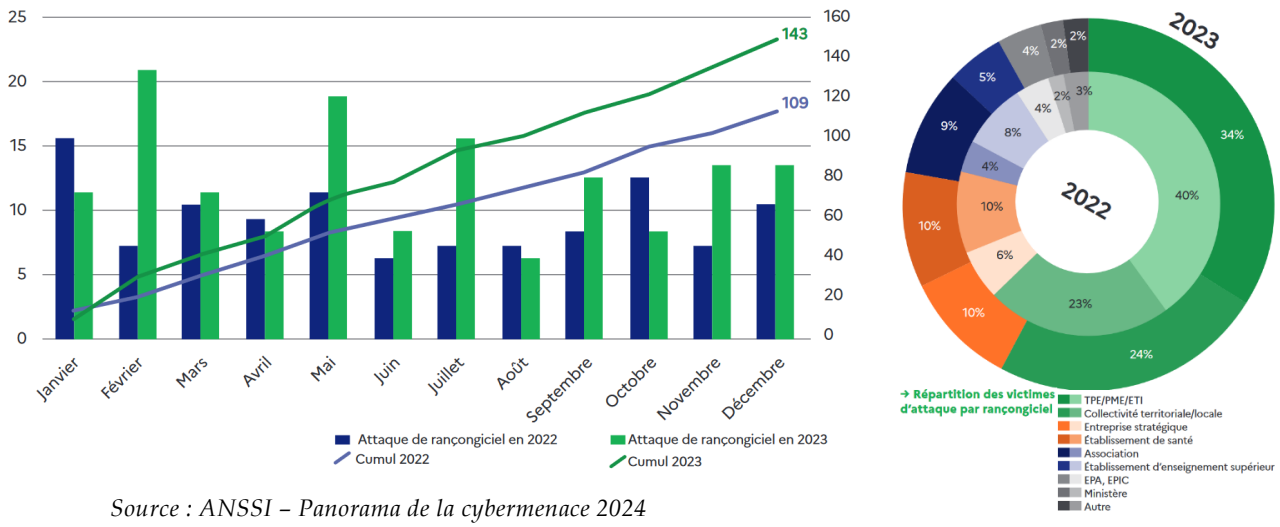
I. UNE AUGMENTATION DU NIVEAU DE LA CYBERMENACE EN 2023 AVEC COMME PRIORITÉ LA SÉCURISATION DES JEUX OLYMPIQUES DE PARIS 2024

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 %).

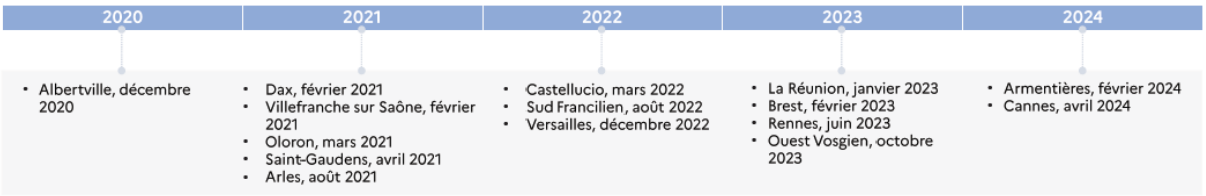
Évolution et répartition des attaques par rançongiciels



Source : ANSSI – Panorama de la cybermenace 2024

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 POUR LES SERVICES DU SGDSN

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.

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).

…/…

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

…/…

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.

II. 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 ETPT 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.

En tout état de cause, les problèmes posés par la contrainte budgétaire n'entraineront aucune rupture capacitaire selon le directeur général de l'ANSSI, mais plutôt l'étalement dans le temps de certains projets.

Plus largement, les missions de l'ANSSI devront par ailleurs être précisée dans le cadre de l'examen par la commission spéciale sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité en cours d'examen au Sénat.

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).

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 certains programmes de coopérations européenne et internationale. Le déficit de 12 postes en 2025 par rapport à la

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

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.

Il reste que les résultats et la motivation des équipes observés permettent de penser que **la France dispose d'une capacité de premier niveau pour s'adapter et relever les défis en matière de cybersécurité et de lutte contre les désinformations**. A cet égard, les rapporteurs se félicitent de l'élaboration pour le courant de l'année 2025 d'une **nouvelle stratégie de lutte contre les manipulations de l'information** portée par une recommandation de la commission d'enquête précitée.

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

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

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**[1].

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

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[2] ;

- 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

[1] *Recommandation déjà formulée dans le cadre du rapport pour avis n° 130 (2023-2024), tome IX, du 23 novembre 2023 : « **il y aurait tout lieu de s'interroger sur la sincérité de la prévision budgétaire et donc sur le principe d'une hausse du socle de dotation des fonds spéciaux** ».*

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

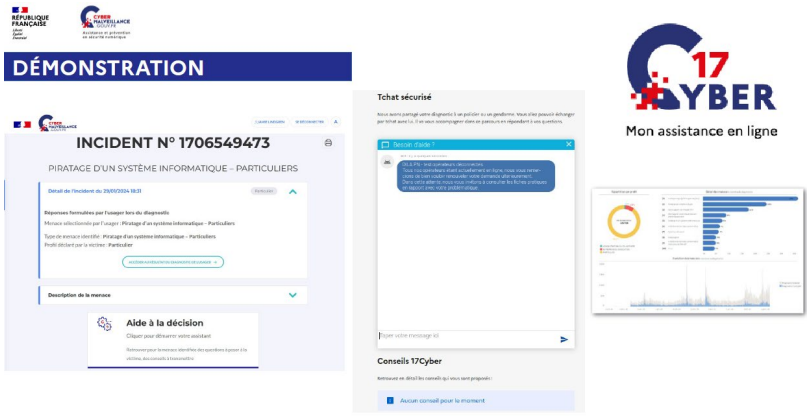
assurer le développement et l'exploitation sur des volumes importants de données (*big data*).

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 »[1]. 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

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

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 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.

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

En dépit de ces problématiques de gouvernance et aléas de la situation politique, **il convient de saluer la conduite à son terme par le GIP Acyma, dans le budget et les délais impartis, d'un projet dont la mise en œuvre est dorénavant effective conformément aux recommandations formulées par vos rapporteurs**[1].

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, cette trajectoire venant en contrepoint de l'accroissement ces dernières années des 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.

Les rapporteurs signalent qu'une telle trajectoire conduirait nécessairement l'institut à reconsidérer ses missions et ses objectifs pour sécuriser son budget à l'avenir, dans un contexte de réduction généralisée des crédits, la problématique n'étant pas tant la baisse des moyens sur 2025 que le risque d'engrenage triennal qu'elle risque d'engendrer.

---

[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.*

Toutefois, **la situation de l'IHEDN a fait l'objet d'un large débat en commission**, le président de la commission rappelant que la fonction stratégique d'influence de cet établissement 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 (*cf. infra*).

* * *

CONCLUSION DES RAPPORTEURS

Compte tenu de l'ensemble de ces observations et des contraintes budgétaires identifiées par les rapporteurs, **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.

Néanmoins, **les rapporteurs entendent souligner que l'avis de rejet prononcé par la commission sur ces crédits du programme 129 ne doit pas altérer le consensus habituel de la commission 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**.

Ils ont ainsi pu s'assurer lors de leurs visites, dans les locaux et au contact des équipes opérationnelles de l'ANSSI, de Viginum et de Cybermalveillance, de la pleine mobilisation des équipes et de leurs capacités à relever les défis de l'année 2025. **Que ces services soient pleinement assurés du soutien et de la vigilance des rapporteurs sur l'exécution budgétaire de l'exercice 2025 et l'allocation des moyens nécessaires à leurs missions**.

TRAVAUX EN COMMISSION

I. EXAMEN DU RAPPORT POUR AVIS EN COMMISSION

Au cours de sa réunion du mercredi 20 novembre 2024, 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. – Monsieur le Président, Chers Collègues, nous avons entendu ici même en audition publique le Secrétaire général de la défense et de la sécurité nationale (SGDSN) avec les responsables des deux principaux services à compétence nationale dont il a la charge : le directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et le chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum).

Je ne reviendrai donc pas en détail sur les motifs de satisfaction de l'année 2024 concernant la lutte contre les attaques cyber et les ingérences numériques étrangères pour lesquelles nous avons collectivement félicité les services concernés.

Avec l'examen du budget du programme 129 dédié à la coordination du travail gouvernemental, c'est l'année 2025 et l'avenir qui nous préoccupent plus particulièrement avec mon collègue co-rapporteur Michaël Vallet.

À cet égard, je remercie le SGDSN pour sa franchise concernant la contraction des moyens que subira ce programme budgétaire et les choix que ses services devront opérer pour s'adapter. Je les rappelle pour que nous ayons ces chiffres à l'esprit : avec 425 millions d'€ au lieu de 438 millions d'€, 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'€ en 2025 au lieu de 76 millions d'€ en 2024) et le Groupement interministériel de contrôle (GIC) qui centralise les techniques de renseignement.

Très concrètement les services du SGDSN (principalement l'ANSSI et Viginum) vont devoir fonctionner avec 8 millions d'euros en moins ;

Quant aux effectifs, le plafond d'emplois ne devrait pas évoluer : il reste à 1284 équivalent temps plein (ETP) ainsi que l'a précisé le SGDSN.

Ce contexte nous a conduit à privilégier cette année la méthode du contrôle sur place et sur pièces pour mieux nous rendre compte de la contrainte qui pèsera sur les missions du SGDSN.

S'agissant des services et des opérateurs nous nous sommes rendus aux sièges opérationnels de l'ANSSI, de Viginum et du GIP Acyma qui opère la plateforme Cybermalveillance. À cet égard, mon collègue Michaël Vallet a prévu de revenir plus en détail sur nos observations.

Nous avons également tenu cette année à entendre directement des acteurs de la cybersécurité (Orange cyber défense et plusieurs entreprises du secteur) mais aussi les cibles des attaques dans le secteur hospitalier et universitaire : l'AP-HP et l'université Paris-Saclay.

Concernant la réduction des moyens de l'Institut des hautes études de la défense nationale (IHEDN), le Général de Courrège, nouveau directeur de l'Institut, nous a confirmé une réduction d'effectif de 5 emplois dès 2025 pour une réduction totale de 17 emplois sur trois ans, soit près de 24% des effectifs actuels qui s'établissent à 71 (ETP).

L'argumentaire développé pour obtenir le maintien des effectifs s'appuyait sur des actions réalisées. Mais il ne s'appuyait pas sur l'atteinte d'objectifs pertinents. Compte tenu de l'évolution de nos finances publiques, l'IHEDN gagnerait à s'interroger sur sa raison d'être et à se concentrer sur ses activités stratégiques pour sécuriser son budget à l'avenir.

Dans un contexte de réduction généralisée des crédits, il me paraitrait raisonnable que chacun agisse en responsabilité et cherche à redimensionner les services pour qu'ils restent efficaces, plutôt que de porter une appréciation destinée à sanctuariser plutôt tel budget que tel autre.

Viginum devait passer de 42 à 65 ETPT, il restera à 42.

L'ANSSI avait demandé 35 millions d'€ et 60 ETP 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 NIS2 ; il n'aura que 27 millions d'€ et zéro ETP en plus ;

Selon l'étude d'impact de la directive NIS 2, ce sont 15 000 entités dans 18 secteurs d'activités, contre 500 dans 6 secteurs pour NIS 1, qui entrent directement dans le champ d'application de cette directive. Mais dans sa mise en œuvre, ce nombre pourrait être multiplié par 2 ou 3, voire plus car les fournisseurs ou prestataires des 15 000 entités initiales pourraient être soumis aux contraintes de la directive par voie contractuelle. Le coût pour les entités concernées de mise en conformité avec les mesures envisagées n'est pas précisé par l'étude d'impact.

Dans une note de présentation d'une version antérieure du projet de loi communiquée aux ministères en mars dernier l'ANSSI estimait à 400 000 € le coût moyen de mise en conformité pour une entité, quelle qu'elle soit — ce

qui représenterait donc un coût global de 6 milliards d'€ pour les seules entités entrant directement dans le champ d'application du texte — et envisageait une subvention moyenne de 25 % pour les collectivités territoriales concernées, ce qui supposerait un budget global triennal de 60 millions €/an.

L'ANSSI devra mieux expliquer comment elle compte répondre à la mise en application de la transposition de la directive NIS 2.

Les missions de l'ANSSI n'étant plus précisées dans le projet de loi qui nous a été soumis, il reviendra à la commission spéciale d'obtenir ces précisions.

De plus, notre commission aura à se prononcer sur une probable réduction supplémentaire de crédit que le Gouvernement demandera au Sénat. Le Gouvernement avait en effet déposé un amendement de réduction supplémentaire de 25 millions d'€ de crédits sur le programme 129, avant que la première partie du projet de loi de finances ne soit rejetée. Cet amendement n'a donc pas été examiné à l'Assemblée nationale mais il risque très certainement de revenir au Sénat.

Plus largement, cette question de moyens pose la question de la gouvernance et des missions. On ne peut pas résoudre un problème ponctuellement pour un service indépendamment des autres. Cela nécessite de revoir les objectifs et les missions assignées à tous les services du Premier ministre : ANSSI, Viginum et les opérateurs y compris Cybermalveillance et l'IHEDN.

M. Mickaël Vallet, rapporteur. – Olivier Cadic a évoqué la question des moyens et je vais revenir sur le bilan et les observations que nous avons pu faire lors de nos différentes auditions et visites de site, notamment sur la question des Jeux olympiques et le panorama de la cybermenace, comme nous le faisons tous les ans, avant de revenir sur les enjeux de gouvernance.

Je tiens donc tout d'abord à saluer la réussite de tout l'écosystème cyber et à sa tête l'ANSSI pour le bon déroulement des JOP alors que le niveau de menace était supérieur à celui de Tokyo. Et même largement supérieur avec 55 milliards d'attaques répertoriées par ATOS, en charge du consortium numérique et cyber, contre moins de 5 milliards aux JO de Tokyo en 2021. Cette réussite est notamment liée à l'efficacité et la rapidité des échanges entre les différents opérateurs concernés par l'évènement comme ATOS et Orange Cyberdéfense. 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 mobilisés pendant l'événement, nécessitant la formation d'agents non spécialistes à la gestion des notifications d'alertes cyber.

S'agissant du panorama des menaces, les chiffres données 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 en ne comptabilisant que les opérations notables qui regroupent elles-mêmes une multitude d'attaques individuelles. C'est notamment le cas des attaques par saturation des réseaux. Je précise qu'il faut faire attention aux chiffres qu'on entend, car il faut comprendre qu'un événement comptabilisé par l'ANSSI peut recouvrir des milliers ou des centaines de milliers d'attaques individuelles tous azimut pour saturer des installations. Ce que je veux relever, c'est 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 à la hauteur.

Dans un contexte marqué par de nouvelles tensions géopolitiques, la cybermenace a continué à évoluer. En 2023, 3 703 événements de sécurité contre 3018 en 2022 ont été portés à la connaissance de l'ANSSI dont 1 112 concernait des incidents contre 832 en 2022.

Les attaques à but lucratif se maintiennent à un niveau élevé avec un nombre d'attaques par rançongiciel supérieur à 30 % par rapport à l'année précédente. Les cibles sont également de plus en plus diversifiées.

À titre d'exemple, le secteur du social est de plus en plus ciblé et devient une source d'inquiétude (exemple : en février 2024, deux opérateurs de gestion du tiers payant ont été victimes d'une cyberattaque affectant les données personnelles de plus de 33 millions de personnes). Ce secteur ne devra pas être négligé dans le cadre de la transposition de la directive NIS 2. Le niveau de maturité des universités et des hôpitaux en matière de cybersécurité demeure très bas, hormis 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. Il faut savoir que ce qu'on a pensé être une cyberattaque sur l'AP-HP cet été a en réalité été une panne d'électricité. C'est très loin d'être le cas dans le secteur hospitalier dans son ensemble mais aussi pour le secteur universitaire et de la recherche, dont nous avons entendu le vice-président en charge du numérique de l'Université Paris-Saclay.

Sur la gouvernance, je reviendrai sur nos visites du GIP Acyma, de Viginum et de l'ANSSI en faisant une observation générale valable pour ces 3 entités, à savoir un manque global de lisibilité des données annuelles dans le plan annuel de performance du SGSDN qu'il s'agisse de la répartition des crédits de personnels ou de la projection pluriannuelle des crédits.

Je formulerais deux constats concernant la plateforme cybermalveillance :

- La mise en place d'un filtre anti-anarques a été autorisée par la loi SREN de 2024. Alors que ce filtre devait être fonctionnel pour les JOP, l'appel d'offres lancé par Bercy (via la DGE) concernant le développement et la gestion du filtre est toujours en cours. Nous pourrions nous émouvoir du fait

que 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 toujours pas été lancée alors qu'elle est prête depuis mars de cette année. Le lancement de cette plateforme devient urgent car elle pourra pallier la disparition de certains centres de réponse cyber régionaux qui arrivent au bout de leur financement par le plan France Relance en 2024 et qui ne seront probablement pas conservés par un certain nombre de régions. Surtout, alors qu'il s'agissait d'une priorité annoncée pour contribuer à la sécurisation des JO, la plateforme n'a toujours pas été inaugurée par le ministre de l'Intérieur qui assure la tutelle de ce dispositif. Il y a toujours urgence et il convient donc de le signaler au ministre actuel.

Concernant Viginum, il faut signaler que pour la première fois depuis sa création en 2021, le budget de VIGINUM ainsi que ses effectifs ne vont pas augmenter. Une telle stagnation nous paraît inquiétante alors que les manipulations de l'information continuent de croître quantitativement et qualitativement grâce notamment à l'intelligence artificielle.

L'ANSSI va également devoir faire face à une forte contrainte budgétaire : elle devra renoncer à 8 millions d'euros (par rapport aux 35 millions de besoin initial) et elle ne pourra pas recruter d'agent supplémentaire (par rapport aux 20 ETPT supplémentaires prévus). Contrairement à ce qu'on nous dit, c'est compliqué de faire mieux avec moins. Cette contrainte budgétaire emporte nécessairement des renoncements de la part de l'agence sur divers sujets :

- 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.

Par ailleurs, l'élection récente de Donald Trump est un signal d'alerte pour l'ANSSI qui, selon nous, devra s'interroger sur son niveau de coopération futur avec les agences cyber américaines. Face à l'extraterritorialité du droit chinois, l'ANSSI devra également rester très vigilante à ce que des données et des matériels critiques restent bien dans l'escarcelle d'opérateurs français.

S'agissant de la transposition de la directive NIS 2, celle-ci élargit considérablement le nombre d'acteurs soumis à des obligations en matière de cybersécurité par rapport à NIS 1. Nous pouvons déplorer l'absence de

réalisation d'un bilan préalable de NIS 1. C'est une maladie française que l'absence d'évaluation avant de passer à l'étape suivante.

Cette observation n'est pas anodine sur le plan des moyens quand on sait que malgré les fonds spécifiquement attribués à la sécurisation des JOP (12 millions d'euros), l'Agence a dû sacrifier 30% de ses autres activités d'audit et d'accompagnement au profit des JOP. Par ailleurs, elle a dû mobiliser 100% de ses équipes pendant l'évènement, s'obligeant à former des salariés non spécialistes à la gestion des notifications d'alertes cyber.

Il me semble par ailleurs important que l'ANSSI fasse un travail d'estimation du coût associé à chaque mesure de sécurité que les entités concernées par NIS 2 devront mettre en place. D'autant plus que les collectivités territoriales seront également concernées.

Nous nous pencherons lors de l'examen du projet de loi sur le projet de l'ANSSI de ne pas sanctionner des manquements à la directive NIS 2 pendant une durée de trois années à compter de la transposition du texte ; ce qui pourrait laisser impunis des graves dysfonctionnements de la part des entreprises concernées, surtout si elles étaient déjà soumises à NIS 1.

Pour conclure, je voudrais rappeler que plus généralement la coordination interministérielle en matière de défense et de sécurité nationale doit s'intégrer dans une stratégie commune à tous les ministères concernés et bénéficier d'un portage politique plus affirmé. J'ai mentionné l'absence d'impulsion politique en ce qui concerne le 17Cyber. Cette question se reposera lorsqu'il faudra porter la révision de la stratégie de cybersécurité et lancer une nouvelle stratégie en matière de lutte contre les manipulations de l'information qu'on nous a promise pour 2025.

Au bénéfice de ces observations, nous vous proposons l'adoption des crédits de la mission *« Direction de l'action du Gouvernement »* mais en regrettant la baisse des moyens sur ces sujets si sensibles qui ont des effets extrêmement concrets dans le quotidien de la population.

M. Cédric Perrin, Président. – Je remercie les rapporteurs.

M. Pascal Allizard. – Je remercie nos collègues pour ce rapport extrêmement clair. Ma question porte sur l'intervention de notre collègue Olivier Cadic car je n'ai pas bien compris sa charge ou son propos concernant l'IHEDN et un certain nombre d'institutions qui rentrent dans le périmètre. Dans cette commission nous portons un principe que le Président rappelle à juste titre qu'il faut essayer de gagner la guerre, avant la guerre, et les outils dont vous nous parlez ce matin sont des outils d'influence qui permettent de travailler à cette mission. Je m'interroge sur le fait que nous votions les crédits en l'état. Peut-être aurions-nous pu envisager comme pour l'audiovisuel public et France Média Monde de réfléchir à un amendement. D'ailleurs notre collègue Mickaël Vallet ne l'a pas complètement dit mais est resté ouvert dans sa conclusion. Je suis donc perplexe sur le propos concernant l'IHEDN, que

j'ai deux bonnes raisons de connaître, car j'ai été auditeur en 2008 et que je représente le Sénat au conseil d'administration.

L'institution a-t-elle failli dans sa mission ? Et si tel n'est pas le cas je ne cache pas que je suis tenté de m'abstenir sur ce rapport.

Mme Hélène Conway-Mouret. – Je suis d'accord que la situation budgétaire appelle des efforts mais je n'adhère pas à toutes les économies surtout quand je pense qu'elles ne sont pas justifiées. J'ai déjà questionné le ministre des armées, dont ce n'est pas les compétences puisque l'IHEDN relève du Premier ministre. Je pensais que le ministre au vu du rôle de l'Institut de rassembler et préparer des hauts fonctionnaires, des militaires et des civils, dont j'ai fait partie comme plusieurs d'entre-nous, pouvait également prendre position. J'ai bénéficié des enseignements de l'IHEDN pas seulement sur le plan professionnel mais également personnel. C'est une entité conçue en 1936 qui a un vrai rôle compte tenu de l'importance d'une mobilisation globale, comme le rappelait tout à l'heure Roger Karoutchi, où nous avons besoin de toute la population. La mission de l'IHEDN, c'est une pédagogie sur la préparation et la conduite de la guerre pour les non militaires. C'est la deuxième fois que l'institut est visé par des économies à réaliser. D'autres instituts ont disparu et dans ce cas si l'IHEDN perd de son attractivité, au regard du coût des formations, il sera remplacé par quoi ? C'est une tentation du moment de démembrer des institutions qui existent depuis des décennies pour les remplacer par autre chose. Donc quelles économies faisons-nous ? Il y a maintenant une académie des hautes études diplomatiques qui n'existait pas et nous avons créé une académie de l'École militaire qui n'existait pas non plus. Cela coûte. Donc je ne vois pas où sont les économies si elles sont transférées vers d'autres postes, sauf à vouloir remodeler tout ce qui existait avant 2017.

M. Rachid Temal. – Je partage les propos de mes deux collègues sur l'importance de cet institut et je précise que je n'y ai pas suivi de formation. On ne peut pas se demander si les élus sont sensibles aux enjeux majeurs qui se profilent et retirer un outil qui fonctionne. Il y a là une contradiction. Je soutiens la démarche d'un amendement.

Le deuxième point que je souhaite aborder est celui des influences étrangères malveillantes sur lesquelles j'ai fait un rapport avec notre collègue Dominique de Legge. Nous avons salué le travail de Viginum et nous souhaitions que le travail de ce service se développe. Or le Gouvernement décide de lui couper les ailes. On ne peut pas voter ce dispositif en l'état car c'est encore une incohérence. Plus que jamais la guerre informationnelle se répand et nos partenaires, notamment américains et britanniques, citent Viginum comme une référence. Or ce service, c'est seulement 50 ETP, dont une quarantaine sur les opérations. Renforcer ces capacités est un investissement plus que nécessaire, donc je souhaite que l'on puisse faire un abondement de crédits vers un organisme qui a prouvé son efficacité et

dévoilé de nombreuses opérations de manipulation en publiant d'excellents rapports techniques.

M. Ronan le Gleut. - L'IHEDN a pour mission de promouvoir l'esprit de défense et sa force est de rassembler des civils et des militaires travaillant ensemble non seulement sur les enjeux stratégiques, la BITD mais aussi sur des sujets académiques, politiques ou du monde des médias. Les officiers supérieurs qui sont auditeurs du Centre des hautes études militaires participent à la session nationale de l'IHEDN, c'est essentiel car ce seront nos futurs généraux. Face au durcissement de la conflictualité, il est important que les civils en prennent conscience et aucune autre institution que l'IHEDN n'offre ce cadre. C'est pourquoi nous avons besoin plus que jamais de cet institut.

M. Roger Karoutchi. – Je n'ai pas été auditeur de l'IHEDN, mais pourquoi faut-il casser quelque chose qui fonctionne ? L'IHEDN a un rôle essentiel car la société civile doit être mobilisé. Je pense à l'« IHEDN jeunes », c'est un outil performant auprès des étudiants. Faisons en sorte que cette institution de 90 ans continue à bien fonctionner car c'est essentiel pour l'avenir de notre défense.

Mme Valérie Boyer. – Nous discutons ce matin essentiellement de l'influence de la France. Il est absolument nécessaire de développer le lien armée-Nation. On ne peut pas balayer un outil qui fonctionne et qui s'est développé régionalement. Le modèle de l'IHEDN a d'ailleurs été copié pour la justice, la sécurité intérieure et la diplomatie. Je ne souscris donc pas aux propos tenus contre l'institut.

M. Cédric Perrin. – Je redonne la parole à Pascal Allizard que je félicite pour son élection à la présidence de la délégation française de l'assemblée parlementaire de l'organisation pour la sécurité et la coopération en Europe (OSCE).

M. Pascal Allizard. – Merci chers collègues. Au vu des interventions de nos collègues, serait-il possible de suspendre l'examen de ce rapport et d'y revenir la semaine prochaine ?

M. Ludovic Haye. – Je voudrais enfoncer le clou, car il y a des pistes d'économie qui sont néfastes quand elles sont appliquées au mauvais endroit. Le lien armée-Nation évoqué par ma collègue Valérie Boyer s'opère par différents biais : l'IHEDN jeunes par exemple, le service national universel qui va rencontrer de grandes difficultés et le service militaire que nous avons connu qui n'existe plus. Il ne reste plus par défaut que les préparations militaires pour les jeunes qui souhaitent faire un premier pas vers nos armées.

S'agissant de Viginum et de l'ANSSI, je pense que nous avons raté le train des Gafam, alors ne ratons pas celui de l'intelligence artificielle qui est un sujet relié à celui des manipulations de l'information.

Mme Hélène Conway-Mouret. – Je voulais rappeler la présence d'officiers supérieurs qui sont des auditeurs étrangers qui passent un an en France à l'IHEDN. C'est un outil d'influence très important.

M. Cédric Perrin. – Je voudrais ajouter que les missions de l'IHEDN s'inscrivent dans les priorités de la revue nationale stratégique de 2022. Je cite le Président de la République : « je veux qu'en 2030 la France ait conforté son rôle de puissance d'équilibres, unie, rayonnante et influente ». Y concourt l'IHEDN au même titre d'ailleurs que l'ANSSI participe à la cyberdéfense et Viginum à l'influence.

L'IHEDN participe à cette fonction stratégique d'influence. Je voudrais rappeler quelques chiffres concernant les propos du rapporteur sur une nécessité d'introspection de l'Institut. Depuis 2010, les effectifs ont été réduit très fortement, de 111 il y a quelques années à 86 en 2024, dont 15 mises à disposition, soit 71 ETP. C'est une baisse de 22,5 % depuis 2012. Et là on leur réappliquerait une nouvelle diminution de 24 %. On peut donc dire que l'Institut a déjà fait sa réorganisation et son introspection.

Je propose que l'on continue à défendre une continuité stratégique, c'est pour cela que nous avons cette discussion. On a parlé de l'ANSSI, de Viginum et de l'IHEDN, mais ce ne sont pas les seuls. Ce sont des acteurs de l'esprit de défense et de la cohésion nationale, de la lutte contre la désinformation et c'est au nom d'une approche globale qu'il nous faut construire nos outils d'influence.

Je rappelle que l'objet du rapport est de refléter l'avis de l'ensemble de la commission. Donc réfléchissons-y, le cas échéant en reportant si vous le souhaitez. Je consulte les rapporteurs sur ce point, faute de quoi, je pense que nous serons plusieurs à vouloir déposer un amendement en nos noms personnels dans un esprit transpartisan sur ce sujet.

M. Mickaël Vallet. – L'appréciation de mon collègue co-rapporteur sur l'IHEDN lui appartient et il y reviendra. À titre personnel, comme l'a remarqué Pascal Allizard, je ne vois pas d'obstacle à voter le fait que les crédits sont insuffisants et qu'il faut les augmenter. Mais comme disait Lacan, la réalité c'est quand on se cogne. Donc où va-t-on prendre les recettes ?

Ce débat ne doit pas altérer le consensus que nous avons habituellement sur les crédits du programme 129 et les enjeux de cybersécurité.

Sur l'IHEDN, ce que nous dit son directeur, ce n'est pas tant la baisse des moyens sur 2025 que l'engrenage triennal que cela risque d'engendrer de manière conséquente.

C'est ce que j'ai dit pour Viginum et l'ANSSI, ce dernier devant renoncer à certains équipements. Plutôt que de reporter d'une semaine, prenons le temps de régler le sujet aujourd'hui.

M. Olivier Cadic. – Sur le fond, je vis dans un pays, l'Angleterre, où lorsqu'il y a un conflit d'intérêt ou que l'on est concerné, on se déporte. Je regarde cela de manière totalement neutre. J'ai beaucoup de respect pour l'institution. Beaucoup des anciens auditeurs ont rappelé la qualité et l'apport de l'IHEDN. Je ne le conteste pas. La question est qu'il y a des mesures d'économie pour tout le monde du fait de l'état de nos finances publiques. Donc la question qui s'est posée en audition est celle des objectifs et de la mission sur le long terme. Ce sont ces éléments d'analyse que j'attendais et que je n'ai pas eu. C'est pour cela que j'ai appelé à s'interroger sur la raison d'être de l'Institut et à se recentrer sur ses activités stratégiques pour sécuriser le budget de l'IHEDN à l'avenir. Dans une entreprise, quand on a le chiffre d'affaires qui baisse on se pose la question de ses missions. On se reconfigure, c'est cela que j'attendais.

Par rapport à la problématique du programme 129, l'ANSSI, Viginum, comme l'a rappelé Rachid Temal, il y a de vrais besoins. Ce budget est un coup d'arrêt à une mission qui est essentielle comme l'a rappelé sa commission d'enquête. Le développement de Viginum est stoppé. Ce n'est pas à nous de faire ce choix, c'est au Gouvernement. A faire un choix, c'est sur Vigninum que je remettrais des crédits.

M. Olivier Cigolotti. – Il faut le temps nécessaire de la réflexion s'il faut préparer un amendement.

M. Rachid Temal. – Avec Michaël Vallet nous partageons une approche cohérente de cette loi de finances puisque nous ne sommes pas caution de ce budget d'austérité. Sur Viginum, que je connais mieux que l'IHEDN, le rapport que j'ai fait avec Dominique de Legge préconisait d'en renforcer les moyens. Respectons les rapporteurs et je propose que nous portions le message dans l'hémicycle, pourquoi pas au moyen d'un amendement transpartisan.

M. Mickaël Vallet. – Nous pourrions proposer de ne pas adopter les crédits. Ce serait à la commission de prendre position ? C'est ma première question.

Deuxièmement, nous pouvons par avance faire savoir que nous ne serons pas d'accord avec un amendement gouvernemental consistant à aggraver la baisse des crédits de ce programme.

Troisièmement, si nous voulons augmenter les crédits, il pourra y avoir un amendement pour renforcer Viginum, le cas échéant transpartisan, et un autre pour soutenir l'IHEDN.

Sur le reste des analyses, il ne me semble pas qu'il y ait de contradictions sur le bilan des insuffisances que nous avons identifiées.

M. Cédric Perrin. – Les rapporteurs souhaitent-ils amender maintenant, l'idée étant que le transfert de crédit provienne du programme 308 qui finance un certain nombre d'autorités administratives indépendantes.

Mme Hélène Conway-Mouret. – Votre constat est-il celui d'une insuffisance de crédit, ce qui clarifierait la question, et ensuite il y aura un débat en séance sur la base d'un amendement ?

M. Akli Mellouli. – Le problème sera le même dans tous les programmes ou un amendement prévoit de retirer à un programme pour donner à un autre.

M. Olivier Cadic. – Nous avons bien identifié dans le rapport les contraintes causées par ce budget. Je ne vois pas d'inconvénient à ce que la commission se prononce sur cette base. Je ne souhaite pas entrer dans une logique de ponction sur un programme pour en abonder un autre.

M. Cédric Perrin. – Je propose que nous donnions un avis défavorable à l'adoption des crédits du programme 129 puis que chacun prenne ses responsabilités pour déposer un amendement en séance.

La commission a donné un avis défavorable à l'adoption des crédits du programme 129.

II. AUDITION EN RÉUNION PLÉNIÈRE

Au cours de sa réunion du mercredi 6 novembre 2024, , la commission des affaires étrangères, de la défense et des forces armées, sous la présidence de M. Cédric Perrin, président, a entendu MM. Stéphane Bouillon, secrétaire général dde la défense et de la sécurité nationale (SGDSN), Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et de Marc-Antoine Brillant, chef du Service de vigilance et de protection contre les ingérences numériques étrangères (Viginum).

M. Cédric Perrin, président. – Nous poursuivons nos auditions sur le projet de loi de finances pour 2025 en entendant ce matin M. Stéphane Bouillon, secrétaire général de la Défense et de la Sécurité nationale (SGDSN), sur les crédits du programme 129 relatifs à la coordination de la sécurité et de la défense.

Il s'agit ici d'un ensemble de moyens permettant au SGDSN d'assurer ses trois missions principales, à savoir l'organisation des conseils de défense et de sécurité nationale, la coordination interministérielle pour prévenir les crises et, enfin, la sécurité des systèmes d'information et la protection contre les ingérences numériques étrangères.

Vous disposez à cet effet de deux services à compétence nationale, dont les chefs vous accompagnent aujourd'hui. Il s'agit de M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information (ANSSI), qui est auditionné pour la première fois par notre commission depuis sa nomination en janvier 2023, et de M. Marc-Antoine Brillant, chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum).

J'ajoute que vous assurez la tutelle de l'Institut des hautes études de défense nationale (IHEDN), bien connu de nos collègues. Je le précise car je ne doute pas que vous serez interrogé à son sujet en raison de la réduction brutale de ses moyens qui est envisagée pour les années à venir.

Nous attendons donc que vous nous présentiez votre budget pour 2025 en nous expliquant précisément les différences entre ce que vous escomptiez pour accompagner la croissance de Viginum et la réalité de l'enveloppe qui vous est allouée. Avec 425 millions d'euros au lieu de 438 millions d'euros, les crédits de paiement de l'action 2 « Coordination de la sécurité et de la défense » subiront en 2025 une baisse de 3 % par rapport à 2024. Vous nous direz quelles contraintes ou renoncements cette évolution impose.

Cette situation est paradoxale car nous savons combien l'année 2024 a mobilisé vos services, tant en matière de cybersécurité que de lutte contre les menaces informationnelles pour assurer le bon déroulement des élections européennes et législatives ainsi que des Jeux olympiques. Elle l'est d'autant plus que l'année 2025 devrait entraîner un accroissement de l'activité de l'ANSSI et de Viginum. Je pense au projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, pour l'examen duquel le Sénat va créer une commission spéciale. Je pense aussi à la préparation d'une stratégie nationale de lutte contre les manipulations de l'information, que la commission d'enquête sénatoriale sur les politiques publiques face aux influences étrangères appelait de ses vœux. Je ne reviendrai évidemment pas sur les évènements de cette nuit aux États-Unis, qui ne devraient pas améliorer la situation en matière de lutte informationnelle et de coopération dans un certain nombre de domaines qui vous concernent plus particulièrement, mais peut-être nous en direz-vous quelques mots.

Mes collègues auront certainement beaucoup de questions à vous poser, à commencer par Olivier Cadic et Mickaël Vallet, rapporteurs pour avis du programme 129.

Je rappelle que cette audition fait l'objet d'une captation vidéo retransmise sur le site internet et les réseaux sociaux du Sénat, puis consultable en vidéo à la demande.

M. Stéphane Bouillon, secrétaire général de la Défense et de la Sécurité nationale. – C'est pour nous un devoir républicain que de venir vous présenter comme chaque année le bilan et les orientations du SGDSN dans son ensemble et dans ses composantes opérationnelles.

S'agissant du bilan, l'impeccable déroulement des Jeux olympiques et paralympiques de Paris a bien sûr constitué notre résultat le plus marquant en 2024. Il s'agissait de notre priorité. Nous y avons travaillé en lien étroit avec la délégation interministérielle aux Jeux olympiques et paralympiques (DIJOP) pendant plus de deux ans, à la fois en tant qu'opérateurs et au titre

de la coordination interministérielle dans le champ de la défense et de la sécurité nationale.

Tout s'est bien passé – ou presque – dans notre champ d'action comme dans tous les autres et nous en sommes fiers. Le succès de la gestion de la sécurité et de la cybersécurité des Jeux a permis l'esprit de fête qui a régné à Paris et sur tous les sites de compétition cet été, l'engouement du public pendant les épreuves et le formidable bilan de nos athlètes, grâce à la mobilisation de tous, acteurs publics, acteurs privés et citoyens.

Heureusement, car certains incidents étaient inquiétants : les trois attentats qui ont été déjoués par la direction générale de la sécurité intérieure (DGSI) au printemps, directement en lien avec les Jeux olympiques ; l'individu d'origine russe qui s'est blessé en manipulant des explosifs dans un hôtel de Roissy-en-France le 3 juin ; les sabotages sur l'infrastructure des lignes à grande vitesse le 26 juillet, le jour même de l'ouverture des Jeux ; et le nombre de manœuvres de désinformation pour dissuader les visiteurs et déstabiliser notre société, qui a largement crû depuis l'automne 2023.

Le rehaussement de nos boucliers cyber a été très utile car plusieurs attaques pour espionner ou saboter des infrastructures critiques ont été constatées. Tous ces dispositifs nous ont également été précieux pour les élections européennes et législatives. Ils étaient déjà en place lors des élections européennes, ce qui nous a permis d'être efficaces. Compte tenu de la surprise qu'a constitué pour beaucoup de monde, y compris pour nos adversaires, la dissolution de l'Assemblée nationale, les élections législatives ont été moins attaquées.

Au SGDSN, nous nous sommes particulièrement intéressés à l'organisation de la gouvernance de la sécurité des Jeux pour vérifier sa pertinence. Tout le champ devait être couvert. Chaque entité, dans le cadre de ses compétences, devait pouvoir disposer d'une structure d'information et de décision opérationnelle, mais il fallait aussi éviter les redondances et les concurrences entre les différents centres de commandement – il y en avait beaucoup – et, pire, une mauvaise coopération.

Dans cette perspective, nous avons monté au printemps un exercice qui a permis de valider le dispositif mis en œuvre. De fait, ces centres, Paris 2024, les collectivités territoriales, les services publics et l'État ont travaillé ensemble de façon fluide, bien coordonnée, sous l'égide du délégué interministériel aux Jeux, du préfet de police, des préfets de Paris et des départements concernés et du Centre national de sécurité des Jeux au niveau ministériel. Ils ont été efficaces et cette leçon nous sera utile pour le futur. Mes services ont également élaboré un bilan des actions menées pour ce qui concerne le SGDSN en lui-même.

S'agissant de la protection et de la sécurité de l'État, la direction en charge a conduit très en amont une politique de préparation des acteurs à la gestion de crise et à l'anticipation. Elle a conçu des outils d'aide à la décision

avec une doctrine, des scénarii de crise et un mémento pour travailler efficacement en cas de crise, organisé des exercices pour les valider, géré la sécurisation des réseaux à tous les niveaux – réseaux électriques, de télécommunications, y compris par satellite, de distribution d'eau et de paiement électronique –, mené des expérimentations technologiques, notamment dans la détection de matières nucléaires, radiologiques, biologiques et chimiques (NRBC) et la surveillance des drones, surveillé la formation de centaines de chiens à la détection d'explosifs et assuré la veille pendant les Jeux, se tenant prête à contribuer, en cas de besoin, à une cellule interministérielle de crise au service du Premier ministre.

En tant que chef de file national pour la cybersécurité, l'ANSSI a mené un important travail de diagnostic et de prévention pour la protection des systèmes d'information des principaux acteurs des Jeux, très en amont. Les vulnérabilités des systèmes ont été testées – et c'est heureux, car il y avait du travail – et corrigées. Des sondes ont été placées aux bons endroits, tandis que des pare-feux ont permis d'entraver de nombreuses attaques à temps. Au total, le relèvement de nos défenses a permis d'éviter ou de limiter beaucoup d'attaques.

Pour cela, l'ANSSI a veillé à l'excellente coordination entre acteurs publics et privés nationaux, européens et internationaux. Peu d'entre eux se connaissaient avant d'entrer dans la préparation des Jeux et cette expérience va nous permettre, grâce à la collaboration et à la confiance établies à cette occasion, de faciliter, par exemple, l'application de la directive NIS 2, dont le projet de loi de transposition en droit français vous a été soumis.

Concernant la lutte contre les manipulations de l'information, Viginum a démontré au public que les acteurs étrangers habituels de la désinformation ont tenté de nuire à nos intérêts fondamentaux en présentant une France incapable d'assurer le bon déroulement des Jeux, car en proie à des émeutes, à l'insécurité et au terrorisme et envahie par les punaises de lit. Des autocraties ont aussi tenté d'instrumentaliser les Jeux pour obtenir des avantages géopolitiques dans le cadre des conflits en cours.

En juillet, l'ANSSI a réussi à bloquer une attaque qui visait à prendre le contrôle de l'ensemble des panneaux d'informations variables en France. Des actions ont aussi été conduites pour faire face aux systèmes autocratiques, beaucoup plus organisés et directifs, laissant moins de place à l'initiative privée que le nôtre.

Dans ce cadre, Viginum a su travailler étroitement avec d'autres services de l'État, dont la préfecture de police de Paris, la DGSI, le ministère de l'Europe et des affaires étrangères, le ministère des sports et le ministère des transports, ainsi qu'avec beaucoup de partenaires étrangers pour faire face à ces opérations. Nous avons, dans ce domaine, une excellente coopération avec les uns et les autres.

Je ne veux pas oublier le travail de l'opérateur des systèmes d'information interministériels classifiés (OSIIC), qui s'est employé à ce que toutes les autorités puissent à tout instant communiquer entre elles, en toute discrétion et où qu'elles soient.

L'excellent bilan sécuritaire des Jeux tient sans doute tant à cette préparation en amont qu'à la mobilisation exceptionnelle et historique de notre pays, avec le concours de ses alliés, non seulement pour la sécurité, mais aussi pour l'accueil et l'hébergement des athlètes et des spectateurs, leur transport et leur santé. Je mesure ce succès aux félicitations sincères reçues de nos amis britanniques, qui ont organisé les Jeux en 2012, et américains, qui les organiseront en 2028. Ces Jeux sont ainsi l'illustration de ce que notre pays, qui doute si souvent de lui-même, est capable de construire et de réaliser. En ces temps difficiles, cela peut donner confiance.

S'agissant de l'état de la menace, j'ai relu, pour préparer mon propos, le compte rendu de mon audition l'année dernière. Je n'ai hélas pas grand-chose à en retrancher. Au contraire, les menaces s'accroissent et nous sommes mobilisés face à elles. Bien sûr, l'élection de Donald Trump aux États-Unis cette nuit va rebattre toutes les cartes. La Russie impérialiste gagne des points dans sa guerre en Ukraine sur le plan militaire, sur le plan diplomatique – grâce aux BRICS, qui ont rompu son isolement – et sur le plan économique – grâce au contournement des sanctions et à sa résilience. Dans ce domaine, que va faire Trump ? Comment et quand cette guerre prendra-t-elle fin ? Quelles en seront les conséquences pour l'Europe ? Nous entrons évidemment dans une période très complexe.

J'ajoute qu'en Afrique, la Russie continue à acquérir de l'influence grâce à la manipulation de l'information et à sa présence militaire. Même si elle est inefficace contre le terrorisme, elle protège les juntes qui sont arrivées au pouvoir. Par ailleurs, il y a toujours un risque d'embrasement du Proche-Orient autour du conflit entre l'Iran et Israël. Outre le retour de Donald Trump, l'éviction hier du ministre israélien de la défense, Yoav Gallant, aura des conséquences. Tout ceci entraîne un risque de prolifération nucléaire dans bon nombre de pays et de multiplication des conflits régionaux, qui, évidemment, ne peut que nous inquiéter pour les années à venir.

La 29ème Conférence des parties (COP29) à Bakou se présente mal, alors que les manifestations du réchauffement de la planète s'aggravent : incendies, inondations, cyclones de plus en plus ravageurs, pénuries d'eau, etc. Nous en sommes et en serons victimes. Les pénuries d'eau actuelles en Guyane, après celles qui ont touché Mayotte l'an dernier, le démontrent amplement.

Nous travaillons donc plus ardemment sur la réforme de la planification de nos réactions aux crises et aux catastrophes pour la rendre plus lisible et opérante, ainsi que sur la stratégie nationale de résilience afin d'amener l'État, les collectivités territoriales, les entreprises et les citoyens à

se préparer collectivement. Nous en parlerons évidemment dans le cadre de l'examen du projet de loi sur la résilience des entités critiques, en application de la directive européenne sur ce sujet.

Les résultats de l'élection présidentielle américaine vont changer la relation entre les États-Unis et le reste du monde autour de quelques déterminants. Ils sont engagés dans une compétition agressive avec la Chine pour conserver leur leadership mondial, économique et militaire. Dans ce contexte, si j'en crois ce que disait le candidat qui vient d'être élu, le sort des Européens ne constituera pas une priorité. Nous sommes même engagés dans une forme de rivalité économique, comme l'a souligné Donald Trump. L'adoption de l'Inflation Reduction Act par l'administration Biden en était déjà une première traduction. L'annonce par Trump de nouveaux droits de douane sur les importations européennes, sa méfiance envers l'Otan et notre dépendance vis-à-vis des États-Unis pour nos approvisionnements en énergie, en matières premières et en métaux rares nous laissent entrevoir, pour la France et pour l'Europe, des temps agités. Évidemment, le SGDSN est très engagé sur ces sujets de sécurité économique, en lien avec le ministère de l'économie et des finances.

L'Europe, elle, se partage entre ceux qui pensent qu'elle doit se renforcer et ceux qui considèrent qu'il n'y a point de salut en dehors de l'atlantisme. Le Parlement européen et la nouvelle Commission européenne vont être confrontés à la recherche d'un nouveau modèle économique, moins naïf et plus souverain, d'autant que l'économie européenne souffre des prises de position passées. Je pense, entre autres, à la fin des véhicules thermiques en 2035, au projet de traité avec le Mercosur et aux taxonomies, certes vertueuses, mais qui entravent nos entreprises.

Le rapport Draghi est un signal d'alarme et, en même temps, un signal d'espoir, dans la mesure où il évoque des pistes pour restaurer notre compétitivité. Mais pour l'instant, nous sommes bel et bien en train de perdre les batailles de l'innovation, de l'intelligence artificielle, du spatial, de l'autonomie alimentaire et de l'autonomie stratégique, alors que le monde se repolarise en blocs ; nous perdons donc progressivement notre souveraineté.

Dans ce contexte, les menaces hybrides se sont renforcées. Attaques cyber et désinformation constituent des armes pour que les autocraties gagnent la guerre sans avoir à combattre. En 2025, le SGDSN veillera encore à une solide coopération interministérielle pour nous en protéger. Les deux stratégies qui sont lancées, l'une en matière cyber, l'autre en matière de lutte contre les manipulations d'information, ont pour objectif de renforcer le travail de l'administration et l'organisation de notre gouvernance et de travailler sur les relations que nous pouvons avoir avec nos alliés pour être plus forts, coordonner nos efforts et renforcer notre protection et notre efficacité dans ce domaine, y compris en s'ouvrant vers le monde académique et l'éducation des citoyens à la cybersécurité ou à la compréhension de ce qu'ils lisent sur les réseaux sociaux, pour mieux se protéger de ces attaques.

Évidemment, nous continuerons à travailler avec nos alliées, les démocraties, qui sont les cibles premières ; nous l'avons vu hier encore aux États-Unis.

Enfin, je ne saurais omettre le risque d'attentat. Même si nous avons levé, dans Vigipirate, un certain nombre de mesures de surveillance et de vigilance adaptées aux manifestations sportives et aux grands rassemblements de public après les Jeux olympiques, le Premier ministre a souhaité maintenir le niveau le plus élevé, urgence attentat, compte tenu de la situation internationale, qui peut catalyser la menace endogène.

Dans ce contexte durablement incertain, le SGDSN est plus que jamais concentré sur ses missions. Elles sont triples : celles qui relèvent du secrétariat des conseils présidés par le Président de la République, le conseil de défense et de sécurité nationale, le conseil des armements nucléaires ou le conseil de politique nucléaire, qui est désormais rattaché, aux termes de la loi que vous avez votée, au SGDSN ; celles qui relèvent de l'animation de politiques interministérielles – et donc du Premier ministre –, comme la planification de sécurité nationale ou l'anticipation des crises – et nous travaillons fortement sur ce qui peut se passer dans les prochains mois et années, la sécurité économique conjointement avec Bercy ou l'instruction des demandes d'exportation de matériels de guerre et de biens à double usage, le rapport qui vous indiquera ce qui a été décidé dans le cadre de la commission interministérielle que j'ai l'honneur de présider devant vous être présenté, je crois, le 26 novembre prochain ; enfin, les missions des opérateurs interministériels dont j'ai parlé.

Dans cette optique, nous avons beaucoup travaillé à la préparation du projet de loi qui vous est soumis et que j'ai cité devant vous à plusieurs reprises, qui transpose trois directives européennes, REC, NIS2 et DORA, et doit nous permettre de renforcer la protection de la Nation et notre résilience collective. La directive REC vise à assurer la continuité d'activité des quelque 300 opérateurs d'importance vitale, c'est-à-dire de ceux qui sont utiles à la maîtrise d'une crise, tandis que la directive NIS 2 porte sur la cybersécurité des 15 000 entités importantes ou essentielles dont l'interruption des systèmes informatiques bloquerait les services aux usagers et entraverait donc lourdement et durablement notre activité et que la directive DORA vise à améliorer la résistance des institutions financières, des banques et des compagnies d'assurance.

Ce projet de loi a été préparé en collant aux plus près aux directives et en évitant la surtransposition, qui est souvent le péché mignon de l'administration française – je ne suis pas sûr, d'ailleurs, qu'il soit mignon –, car elle créerait des inégalités entre nos voisins et nous. Pour autant, il nous dotera d'outils qui seront collectivement très utiles.

Cependant, afin de ne pas peser brutalement sur les opérateurs, la ministre, Mme Chappaz, qui défendra ce projet de loi devant vous, vous proposera que l'application des nouvelles règles de sécurité soit

proportionnée et très progressive. En particulier, le Gouvernement souhaite exempter les collectivités territoriales de sanctions en cas de carence affirmée, puisque leur moteur n'est pas le profit, mais l'intérêt général. J'ajoute que les collectivités regroupant moins de 30 000 habitants seront exemptées d'obligations nouvelles.

Nous veillerons, en liaison avec vous, à mettre en avant la pédagogie et un travail de conviction. En effet, la résilience passe par l'adhésion du plus grand nombre et ne peut être fondée sur la seule contrainte, même si, à un moment, il faut bien imposer à certains de ne pas mettre en danger la sécurité de tous par leurs carences.

J'en terminerai, Monsieur le président, par un mot sur les moyens du SGDSN tels que prévus dans le PLF pour 2025. Comme vous le savez, le Gouvernement a placé la question des finances publiques au cœur de son action. Cela se traduit par des efforts demandés aux services de l'État et aux collectivités et, bien entendu, aux services du Premier ministre en premier chef. Dans ce cadre, les crédits de ces derniers baisseront légèrement en 2025. S'agissant du SGDSN, les moyens pour 2025 seront presque identiques à ceux de 2024. Nous devrons fonctionner avec 307,6 millions d'euros, soit 8 millions de moins qu'en 2024, dont, hors T2, 242 millions d'euros en autorisations d'engagement (AE) et 243 millions d'euros en crédits de paiement (CP). Cette baisse concernera surtout les crédits techniques d'investissement mutualisés (CTIM), qui soutiennent les investissements techniques que se partagent les services de renseignement. Nous compterons 1 284,7 équivalents temps plein (ETP) hors effectifs militaires – qui se montent à 305 – et notre schéma d'emploi pour 2025 ne prévoit pas la création de nouveaux postes.

Nous avons donc pris des mesures pour adapter notre organisation de façon à assurer la continuité des missions importantes. Nous priorisons nos missions et cherchons les économies, mais je peux vous assurer que nous ne serons pas empêchés dans notre cœur de métier.

En revanche, certains projets, notamment en soutien à des partenaires étrangers, devront être réduits ou retardés. Le renouvellement de certains matériels et investissements, notamment immobiliers, sera décalé, ce qui nous obligera sans doute à garder des locaux que nous louons actuellement. Mais dans tous les cas, le SGDSN sera au rendez-vous de 2025, comme il l'aura été en 2024.

Vous avez parlé, Monsieur le président, de l'IHEDN. Après avoir connu une réforme importante au début des années 2020, l'IHEDN fonctionne efficacement et avec beaucoup de succès, puisque les sessions accueillent de plus en plus d'auditeurs, et assure l'information de l'ensemble des corps de la Nation et le rayonnement de notre défense, non seulement en France, mais aussi à l'étranger. Les efforts qui lui sont demandés cette année devront être revus l'année prochaine, mais cela fera partie du débat que nous aurons avec l'IHEDN, le ministère des armées et les services du Premier ministre. En tout

état de cause, le directeur de l'IHEDN m'a indiqué qu'il devrait parvenir à y faire face cette année.

M. Vincent Strubel, directeur général de l'Agence nationale de sécurité des systèmes d'information. – La menace en matière de cybersécurité évolue et s'intensifie, puisque le nombre d'incidents significatifs traités par l'ANSSI a augmenté de près de 30 % entre 2022 et 2023, passant de 832 à 1 112. Je me risque à prédire que l'évolution sera du même ordre, si ce n'est plus, en 2024.

Au-delà de ces chiffres bruts, la menace s'accroît dans notre cœur de métier historique, c'est-à-dire la réponse à la menace stratégique, doux euphémisme pour parler des attaques menées par des États contre nos intérêts les plus fondamentaux. L'espionnage reste ce qui nous occupe le plus, ciblant toujours des entités stratégiques, des administrations sensibles ou des entreprises innovantes ou stratégiques.

Cette menace d'espionnage est toujours aussi présente et se diversifie. Elle touche aussi de nouveaux types d'acteurs, comme les *think tanks*. Nous avons publié un état de la menace sur ces acteurs particuliers – sur les organes de normalisation par exemple. Elle s'étend aussi à toute la chaîne de valeur. Face à des acteurs stratégiques qui se protègent de mieux en mieux, les attaquants savent s'en prendre au maillon faible que sont les prestataires et les sous-traitants. Nous devons donc couvrir une cible de plus en plus large.

L'autre composante de cette menace stratégique étatique, c'est le sabotage, que nous anticipions depuis des années, qui est devenu une réalité parfaitement tangible et qui constitue le quotidien de l'Ukraine depuis des années – sans doute plus que trois ans. Il correspond à la destruction des infrastructures, des opérateurs de l'énergie ou des télécommunications. Kyivstar, opérateur téléphonique majeur de l'Ukraine, a ainsi été totalement paralysé par une cyberattaque. Dans la partie occidentale de l'Europe, nous observons des manœuvres de reconnaissance de la part d'acteurs qui cherchent à mieux cerner les contours de nos infrastructures critiques, voire du prépositionnement, c'est-à-dire une prise de contrôle de la part de ces acteurs, qui s'installent au sein des réseaux de nos opérateurs critiques, sans espionner, et dont nous supposons donc qu'ils sont là pour pouvoir tout éteindre ou tout casser le moment venu, quand on leur en donnera l'ordre.

S'il n'y avait que cette menace-là à traiter, la tâche serait déjà ambitieuse. Malheureusement, l'explosion de la menace systémique constitue l'autre évolution majeure de ces dernières années. Il s'agit d'une menace qui n'est pas ciblée, touche en premier lieu les victimes les plus faciles, est liée au crime organisé et cherche à faire de l'argent au travers du rançongiciel, c'est-à-dire de la paralysie d'infrastructures informatiques et de l'extorsion de rançons pour les libérer.

Ce crime organisé pratique depuis quelques années une pêche au chalut et attrape tout ce qu'il peut. Nos hôpitaux en ont été les victimes les

plus visibles en 2021 et en 2022, avec des situations proprement catastrophiques. Sur ce plan, nous pouvons noter une certaine amélioration : même si nous sommes loin d'être sortis de la zone de vulnérabilité de nos hôpitaux, leur capacité à réagir efficacement face aux attaques s'est nettement améliorée. Nous n'avons recensé qu'un incident réellement grave au cours de l'année écoulée, celui d'Armentières, tandis que beaucoup d'incidents qui auraient pu l'être ont été évités.

Malheureusement, les hôpitaux ne sont pas les seules victimes. Les autres victimes récurrentes de ce type d'attaque restent sur un plateau haut de la menace. Je veux parler des collectivités, avec des catastrophes à Albi ou à Saint-Nazaire – et j'en passe –, et des entreprises de toute nature. Je note par exemple que les médias ne sont pas à l'abri, puisque Libération se débat depuis le week-end dernier avec une attaque de ce type, tandis que les éditions Bayard se sont vues très largement contraintes, y compris dans la publication du quotidien La Croix il y a quelques semaines.

En complément ou en alternative à la paralysie des infrastructures informatiques, ces acteurs du crime organisé se tournent de plus en plus vers le vol de données et l'exigence de rançons contre leur non-publication. La victimologie évolue donc et s'étend désormais aux acteurs du domaine social, qui détiennent des données sensibles dont la publication serait évidemment un évènement problématique que les acteurs concernés cherchent à éviter. Les opérateurs de tiers payant en ont fait les frais en février, au moment où un acteur équivalent du paiement des prestations de santé, Change Healthcare, connaissait une attaque équivalente, voire pire, aux États-Unis. Je pense d'ailleurs qu'il s'agit de la première attaque dont les conséquences financières dépassent le milliard de dollars, puisque le paiement des prestations de santé a été bloqué pendant plusieurs semaines. Cette menace se développe également dans le domaine de l'enseignement supérieur et de la recherche, avec l'exemple de l'université de Paris-Saclay, qui en a été la victime à la fin de l'été.

Nous voyons également de plus en plus d'acteurs revendicatifs du domaine activiste, qui ne font pas nécessairement des choses très graves, mais très visibles et tout de même gênantes au quotidien, notamment dans le contexte géopolitique que nous connaissons, paralyser certains sites web par des attaques de déni de service, c'est-à-dire de simple saturation, comme une opération escargot, et essayer de faire de plus en plus de choses de manière très désinhibée, y compris contre des infrastructures qui pourraient être critiques à grande échelle. Par exemple, certains de ces acteurs, comme la Cyber Army of Russia Reborn, s'en prennent à des micro-installations de production d'électricité ou à des éoliennes pour détruire physiquement ces équipements au travers d'attaques d'une technicité très faible, mais que nous surveillons évidemment de près. Cette évolution de la menace nous amène donc à nous pencher de nouveau sur la protection, avec le travail à venir sur

la directive NIS 2 ainsi que d'autres textes réglementaires que j'évoquerai rapidement.

Nous avons été confrontés à cette menace dans la préparation et la mise en œuvre des Jeux olympiques. En juillet 2022, l'ANSSI a été désignée chef de file de la cybersécurité des Jeux, ce qui a donné lieu à un travail en deux phases : un travail de chef d'orchestre de la préparation pendant deux ans, avec un travail de prévention, d'accompagnement de près de 500 entités jugées critiques pour l'organisation des Jeux, de test et d'amélioration de leur sécurité, d'entraînement ainsi que de communication auprès d'acteurs auxquels, jusque-là, l'ANSSI ne parlait pas : des fédérations sportives, des lieux de compétition, des stades, etc. ; puis, au-delà de ces deux ans de préparation, trois mois de gestion de crise – même s'il n'y a pas eu de crise majeure visible –, durant lesquels nous avons traité en horaires étendus tout ce qui pouvait se passer du 8 mai, date d'arrivée de la flamme olympique, au 8 septembre, date de clôture des Jeux paralympiques.

Tout cela avec des moyens spécifiques de l'ordre de 12 millions d'euros, qui nous ont permis d'industrialiser des prestations de services et des équipements en matière de cybersécurité, mais surtout l'utilisation de 30 % des capacités de l'ANSSI pour la préparation des Jeux pendant deux ans et de 100 %, voire 120 %, de ces capacités pendant les trois mois de la période olympique, puisque l'ensemble des agents de l'Agence, y compris ceux dont le métier n'est pas de gérer des crises cyber, ont été entraînés et mobilisés pendant cette période.

Le résultat fut une victoire sans ambiguïté, ce qui est suffisamment rare dans notre domaine pour le signaler. Aucune cyberattaque n'a perturbé le déroulement des Jeux ni entamé la confiance des délégations, des spectateurs et de nos partenaires internationaux, qui étaient préoccupés par la sécurité de l'évènement.

Pour autant, nous avons tout de même été confrontés à une vague significative d'attaques. L'ANSSI a dénombré 548 tentatives d'attaque, dont 83 ont réussi à produire des effets, la plupart du temps mineurs, mais non nuls, durant la période et sur le périmètre olympiques. Le comité d'organisation ayant compté 55 milliards d'attaques, je tiens à préciser que nous comptons la même chose, mais de manière différente : pour une attaque ou une tentative d'attaque comptée par l'ANSSI, les organisateurs – et c'est légitime de leur point de vue – comptent les milliers d'actions techniques individuelles qui conduisent à cette attaque ou à cette tentative d'attaque. Le volume d'attaques a donc bel et bien progressé de façon significative par rapport aux Jeux de Tokyo.

Pour autant, l'énorme majorité de ces attaques a été bloquée rapidement. L'établissement public de la Villette, qui hébergeait un certain nombre de délégations, et le village olympique, ou l'Accor Arena de Bercy, qui accueillait plusieurs épreuves, ont vu des attaques bloquées très tôt et sans

qu'elles produisent d'effet, grâce à des mécanismes de détection mis en place par l'ANSSI. Nous avons également mené un travail spécifique sur l'assainissement de l'eau, qui a lui aussi constitué une cible pour un certain nombre d'acteurs et a réussi à tenir bon.

Le fait que les attaques soient bloquées très tôt ne nous permet pas toujours de connaître l'identité de l'attaquant ni son intention. Néanmoins, cela me donne à penser qu'à l'évidence, certains en voulaient au bon déroulement des Jeux, dans toutes les composantes de la menace, qu'il s'agisse d'États qui ont organisé des tentatives de sabotage ou d'espionnage, de criminels qui ont cherché à faire de l'argent avec du rançongiciel – le Grand Palais en a fait les frais mais, là encore, sans conséquence sur la compétition – , ou d'activistes de tous genres qui avaient annoncé vouloir s'en prendre à l'assainissement des eaux de la Seine – sans succès.

Au total, donc, les mesures de prévention que nous avons mises en place ont été efficaces. L'équipe de France de la cybersécurité a été d'une efficacité remarquable et c'est une vraie victoire collective. Nous avons aussi fait preuve d'une transparence assez nouvelle, qui a porté ses fruits dans le partage rapide de l'information avec nos partenaires étrangers, mais aussi avec les médias. Je tiens à souligner que nous n'avons pas vu pendant ces Jeux ce que nous avions pu voir précédemment, c'est-à-dire des reprises sans esprit critique de revendications parfois abracadabrantesques de certains groupes activistes, dont ceux qui prétendaient avoir pollué la Seine. C'est l'occasion de signaler une coopération étroite avec Viginum, qui montre toute la pertinence de notre positionnement commun au sein du SGDSN, parce que ces enjeux sont évidemment à la frontière entre la cyberattaque et la manipulation de l'information.

Tout cela est donc très riche en enseignements pour la suite, mais porte également un message d'humilité. En effet, nous avions finalement, dans la préparation des Jeux, une unité de temps et de lieu : nous savions où et quand les attaquants allaient chercher à nous faire du mal. Le problème plus général que nous avons à traiter est toutefois plus complexe.

Pour la suite, il nous faudra apporter des solutions à des petites victimes qui sortent de notre champ de compétences habituel. Nous avons aujourd'hui une capacité reconnue pour faire face à la menace étatique sur nos intérêts fondamentaux, c'est-à-dire les opérateurs critiques et les administrations sensibles.

Je signale au passage que nous le faisons de manière frugale, puisque nous sommes des petits parmi les grands. Nous assumons ces missions avec un peu plus de 600 agents et un budget de l'ordre de 25 millions d'euros, tandis que les Allemands sont trois plus nombreux –1 800 aujourd'hui – et que leur budget est dix fois plus important, de l'ordre de 240 millions d'euros. Il faut le mettre au crédit des agents de l'ANSSI, des pouvoirs dont vous avez bien voulu nous doter de par la loi et d'une organisation qui a fait ses preuves,

en concentrant au-dessus de la mêlée, dans une agence unique, l'ensemble du champ d'intervention de la cybersécurité, même si nous travaillons toujours en étroite coopération avec le secteur privé, autant qu'avec les services de l'État.

Il va désormais nous falloir transformer cette excellence pour en faire bénéficier le plus grand nombre et répondre aux besoins, d'une nature un peu différente, de milliers d'acteurs confrontés à la menace systémique avec la directive NIS 2, dont je signale qu'elle n'est pas la suite logique de la directive NIS 1. Cette dernière, qui est relativement récente, était concentrée sur quelques centaines d'opérateurs absolument essentiels, quand NIS 2 couvre des milliers d'acteurs bien plus petits contre une menace de nature différente, la menace systémique non ciblée. Cela va nécessiter un changement dans le positionnement de l'ANSSI. Il nous faudra trouver le juste niveau d'exigence, pas trop élevé, car il n'est pas envisageable de traiter une PME comme EDF, mais pas trop faible non plus.

Cet enjeu va nous amener à mobiliser plus que jamais cette équipe de France de la cybersécurité qui a remporté la médaille d'or de la cybersécurité des Jeux pour accompagner collectivement ces milliers d'entités dont la maturité cyber reste à construire. Il nous faudra du temps : cela ne nécessitera pas moins de trois ans et nous le ferons dans la pédagogie et la co construction, comme nous le faisons depuis septembre, avec la consultation de 79 fédérations professionnelles – une première à cette échelle pour l'ANSSI – et de 13 associations d'élus.

Je signale dans le même champ réglementaire un autre objet, le Cyber Resilience Act (CRA), un règlement européen d'application directe qui sera le pendant de NIS 2 : là où NIS 2 va réguler les utilisateurs du numérique, le CRA imposera des exigences de base à tous les producteurs de produits numériques sur le marché intérieur européen et équilibrera les responsabilités entre ceux qui utilisent le numérique et portent certaines responsabilités et ceux qui produisent les briques de base du numérique, portent une responsabilité éminente dans les défauts de sécurité constatés et disposent d'une vraie marge de progression justifiant qu'ils soient régulés.

Tout cela se fera également avec la densification de cette équipe de France et des structures de l'écosystème cyber. L'ANSSI travaille par nature en réseau avec des prestataires privés, des services de l'État et de plus en plus de centres de réponse à incidents (CSIRT) dans les logiques sectorielles ou régionales – un modèle qui a bien fonctionné pendant les Jeux olympiques et qui, je l'espère, va se développer dans la préparation du passage à l'échelle.

Nous allons devoir le faire avec une contrainte budgétaire, puisque notre budget pour 2025, hors T2, sera peu ou prou équivalent à celui de 2024, à 27 millions d'euros contre 25 millions d'euros l'an dernier, et une stagnation des effectifs, là où nous estimions avoir besoin d'une soixantaine d'ETP pour prendre en compte l'évolution de la menace et préparer NIS 2.

Il sera donc nécessaire d'accepter quelques renoncements sur l'extension du périmètre de couverture, et notamment la supervision par l'ANSSI du système d'information de l'État, sur le développement de notre expertise dans des domaines émergents comme l'intelligence artificielle, qui sera certainement moins rapide, et sur certaines de nos missions, que nous devrons déprioriser au profit de l'essentiel, c'est-à-dire de notre capacité opérationnelle et de l'accompagnement de la mise en œuvre de NIS 2.

M. Marc-Antoine Brillant, chef du service de vigilance et de protection contre les ingérences numériques étrangères. – L'année dernière, j'avais eu le privilège d'évoquer devant vous la dégradation du contexte géopolitique auquel nous faisions face et qui était notamment caractérisé par une compétition stratégique désinhibée et l'usage décomplexé du rapport de force, avec pour instruments les actions de nature hybride dont la menace informationnelle est l'essence même.

Malheureusement, un an plus tard, le constat reste le même. Deux conflits armés régionaux dont les effets ont largement dépassé les frontières des seuls belligérants persistent, tandis que l'existence de zones de tension, notamment en Afrique et en région Indo-Pacifique, et la poursuite de la contestation du modèle démocratique offrent un terrain d'action très favorable aux acteurs de l'ingérence numérique étrangère. Par ailleurs, les enjeux économiques et technologiques font l'objet d'une véritable bagarre stratégique pour la conquête d'une position dominante ou le rattrapage d'un retard.

Dans ce panorama, qu'en est-il de la menace informationnelle ? Ou plutôt, quel usage nos compétiteurs stratégiques en font-ils ? Je vous parle avec une année supplémentaire de recul : cinq campagnes dévoilées, la fameuse affaire des étoiles de David, la campagne Olympia contre nos Jeux olympiques, le dispositif Portal Kombat, la dénonciation des manœuvres informationnelles en Nouvelle-Calédonie de la part d'acteurs proazerbaïdjanais, la campagne Matriochka, deux élections et des Jeux olympiques ; et je peux affirmer aujourd'hui que la manipulation de l'information est proche de nous.

Pour être plus clair, je vous parlerai d'une menace que je qualifie d'intime, et ce pour plusieurs raisons. D'abord parce qu'elle connaît le fonctionnement de notre démocratie et de notre société et nos lignes de fracture. Il suffit d'observer les élections dans divers pays, y compris en France, pour s'en assurer.

Cette menace est intime parce qu'elle suit notre actualité, s'y intéresse et tente d'exploiter tout fait divers et tout évènement. La situation dans nos territoires ultramarins est parfaitement connue de certains acteurs étrangers qui n'hésitent pas à susciter et à attiser la contestation en trompant volontairement l'opinion publique.

Elle est intime parce qu'elle connaît aussi notre histoire et notre héritage. La tentative d'instrumentalisation de notre débat public sur le sujet des étoiles de David en est un parfait exemple, tout comme les accusations répétées de colonialisme envers notre politique étrangère.

Elle est encore intime parce qu'elle s'attache à nous accompagner dans la durée, avec des modes opératoires de plus en plus persistants. À ce titre, les campagnes RRN, dévoilées l'année dernière, mais aussi Portal Kombat ont démontré leur capacité d'adaptation à nos réponses.

Enfin, cette menace est intime parce qu'elle nous met à l'épreuve en nous imposant de l'humilité et, demain, probablement, des réponses qui ne relèveront pas uniquement du champ régalien, mais davantage de celui de l'éducation, de l'information et d'une meilleure collaboration avec la société civile. C'est d'ailleurs l'objet de la revue stratégique de la lutte contre les manipulations de l'information qui était souhaitée par votre commission d'enquête et dont le pilotage et la conduite ont été confiés au SGDSN.

Si la nature intime de cette menace informationnelle qu'est l'ingérence numérique étrangère est désormais bien connue, elle présente aujourd'hui plusieurs visages, au travers notamment de l'usurpation d'identités d'institutions officielles. Je pense à la DGSI et au SGDSN, mais également à la CIA ou à nos médias. Elle présente un autre visage, qui est celui, bien connu, de l'animation de réseaux de faux comptes pour massifier la diffusion de contenus et générer de faux contenus crédibles grâce à l'usage de l'intelligence artificielle générative, ainsi que celui de l'utilisation d'influenceurs ou de comptes à forte audience pour amplifier la visibilité de certains récits.

Face à ce constat, une question subsiste : celle de l'impact réel de la manipulation de l'information et de ces opérations ou campagnes d'ingérence numérique étrangère. À ce propos, la mesure de l'impact d'une campagne numérique de manipulation de l'information ne fait pas véritablement l'objet d'un consensus académique ou scientifique. Principalement empirique, l'analyse de ce qu'on appelle l'impact consiste bien souvent à relever des indicateurs quantitatifs de visibilité issus des principales plateformes de réseaux sociaux, avec le caractère relatif de ces indicateurs : le nombre de vues, de likes, de partages ou de commentaires. Ceux-ci ne fournissent toutefois qu'une vision parcellaire de l'exposition d'un lectorat ou d'un auditorat à une campagne, sans permettre d'en mesurer les effets sur le long terme. De fait, une approche simplement fondée sur des indicateurs issus de plateformes ne permet de mesurer que partiellement la visibilité de manœuvres informationnelles, puisqu'elle écarte la nécessaire analyse de l'état sociologique d'une population donnée, exposée de manière répétée à un narratif sur un temps long, avec les biais qui peuvent en découler.

À Viginum, nous adoptons donc une posture de prudence s'agissant de la mesure de l'impact d'une campagne. Nous préférons évoquer un risque d'impact, en essayant de faire le lien avec un changement de comportement

dans la population visée et de voir si une campagne numérique produit des effets dans le champ de la vie réelle.

S'agissant de notre action, je vous avais rendu compte l'an dernier d'une activité opérationnelle croissante, avec près de 40 % de détections supplémentaires par rapport à l'année 2022. Concrètement, en 2023, nous avions identifié 230 phénomènes inauthentiques de manipulation de l'information. Pour 2024, je peux vous dire que nous avons dépassé ce nombre au 1er octobre, à la faveur de dispositifs informationnels particulièrement persistants dans notre débat public numérique et très opportunistes. J'évoquais avec vous à ce propos l'instrumentalisation de tout fait d'actualité.

Face à cela, Viginum a directement participé, au cours de l'année écoulée, aux actions de communication stratégique du ministère de l'Europe et des affaires étrangères pour dénoncer cinq manœuvres informationnelles sur la base de rapports réalisés par le service, qui ont été rendus publics.

J'ai mentionné le phénomène des étoiles de David en novembre 2023, mais aussi la campagne baptisée Olympia, qui impliquait des acteurs azerbaïdjanais et visait à dénigrer la capacité de la France à organiser les Jeux olympiques dans de bonnes conditions de sécurité. Je pense aussi au fameux réseau de portails d'information Portal Kombat, que nous avons dévoilé en février 2024. Il reliait 193 portails d'information multilingues ciblant plusieurs pays en Europe et avait finalement une visibilité relativement faible. Nous parlions tout à l'heure de la notion d'impact ; il est intéressant de noter, à cet égard, que 30 jours après nos révélations, les opérateurs de ce dispositif ont déposé de nouveaux noms de domaine pour cibler l'intégralité des pays de l'Union européenne, à deux mois des élections européennes. Le fait de dévoiler provoque donc des effets chez nos adversaires. J'ai également cité les manœuvres informationnelles de l'Azerbaïdjan en Nouvelle-Calédonie au mois de mai 2024, dont l'objet était bien évidemment d'instrumentaliser les émeutes en cours pour décrédibiliser la politique conduite par l'État. Enfin, je n'oublie pas la fameuse campagne prorusse Matriochka, qui visait en particulier les Jeux olympiques. Nous avons, à ce titre, rendu compte au mois de septembre de notre action au travers d'un rapport sur les Jeux.

Par ailleurs, sur le plan de la collaboration, nous avons signé deux conventions avec des partenaires clés. Je pense à une convention avec la plateforme Pharos du ministère de l'Intérieur, qui a permis de nous identifier en tant que signaleur de confiance pour les contenus illicites. Je pense également à la convention que nous avons signée avec l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) au mois de juillet dernier afin de mettre à sa disposition notre capacité opérationnelle et notre expertise technique, au profit de sa nouvelle mission de coordonnateur national des services numériques découlant de la mise en œuvre effective du Digital Services Act (DSA).

En outre, nous avons consolidé nos relations internationales et européennes auprès d'une vingtaine de pays, à la fois dans et en dehors de l'Union européenne, noué des échanges nourris avec l'OCDE et le G7 et concrétisé un engagement extrêmement fort avec les institutions de l'Union européenne. Je pense notamment aux services de la Commission européenne au titre du DSA, mais aussi au Service européen pour l'action extérieure (SEAE).

Enfin, notre souhait est de poursuivre notre ouverture vers la société civile, les médias, le monde académique et l'éducation nationale. En matière scientifique, nous avons publié trois articles de recherche qui ont été réalisés cette année par le service, et notamment par nos data scientists. Nous nous investissons avec beaucoup d'ambition dans le cadre du futur sommet sur l'intelligence artificielle, qui se tiendra à Paris en février prochain. Nous souhaitons pouvoir mieux outiller la société civile et le monde académique avec des outils qui permettent de détecter, par exemple, des phénomènes inauthentiques.

M. Olivier Cadic, rapporteur pour avis. – Je tiens tout d'abord à m'associer aux propos du président pour saluer votre action et celle de vos services au cours de l'année 2024. Vous avez relevé le défi des Jeux olympiques dans un contexte géopolitique extrêmement tendu et rendu encore plus complexe en politique intérieure par la succession des élections européennes et législatives. Je veux donc saluer l'action de l'ANSSI, de Viginum et, évidemment, de tout l'écosystème qui vous accompagnait en première ligne et qui a répondu à ces menaces. En fait, nous pourrions dire que le dôme cyber a tenu.

Je disais l'an dernier qu'il n'y aurait pas de médaille d'argent en cas de défaillance de nos systèmes d'information et de déstabilisation du déroulement des opérations électorales. Il n'en a rien été, malgré des attaques bien réelles, et il faut s'en féliciter. Je pense comme vous, Monsieur Strubel, que vos services méritent une médaille d'or. Il est donc important de leur témoigner toute notre reconnaissance. En tant que sénateur des Français établis hors de France, je souhaiterais en profiter pour exprimer notre gratitude à votre égard pour le bon fonctionnement du vote par internet, devenu incontournable pour organiser une élection réussie à l'étranger et qui s'est avéré très performant.

Ce satisfecit ne doit pas nous empêcher de penser à l'avenir. Or ce budget pour 2025 ne répond manifestement pas aux besoins qui étaient exprimés antérieurement par vos services. L'ANSSI escomptait une croissance de ses effectifs et de son budget afin d'assurer les missions supplémentaires qui lui seront confiées après l'examen à venir du projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier. Au lieu de réguler l'activité d'environ 500 entités, l'Agence devra changer d'échelle pour en gérer environ 15 000. Elle devait poursuivre

sa croissance avec 65 ETP supplémentaires en 2025 ; ce ne sera pas le cas, ses effectifs n'évoluant pas.

Ces deux cas de figure posent la question des priorités et des ajustements que vous devrez assumer ainsi que celle du périmètre des missions de l'ANSSI. L'Agence pourra-t-elle continuer à mener de front ses activités de régulateur, mais aussi d'acteur et parfois de prestataire de sécurité ? Nous ne pouvons pas regarder 2025 sans se projeter dans la suite.

Lorsque nous avons échangé au sujet des attaquants, nous avions dit que le premier pays d'origine de ces derniers était la Chine, le deuxième la Russie et le troisième l'Iran. Viginum agit aujourd'hui comme une force de réaction rapide pour contrer la désinformation. Vous dénoncez et faites du name and shame. Il faut effectivement nommer ceux qui nous attaquent, mais cela n'est pas toujours le cas. J'aimerais donc savoir quelle procédure vous devez suivre pour pouvoir nommer un attaquant.

M. Mickaël Vallet, rapporteur pour avis. – Je m'associe évidemment aux félicitations s'agissant des Jeux olympiques. Nous avons mené plusieurs auditions avec des acteurs privés pour finir par conclure que la menace n'a pas été sous-estimée et que nous ne nous sommes pas fait peur pour le plaisir. Simplement, vous étiez prêts. Nos adversaires ont fait ce qu'ils ont pu avec leurs techniques et le résultat n'en a pas été l'absence d'attaque ou de pénétration, mais l'absence d'impact, comme vous dites, ou de conséquences.

Vous avez évoqué, Monsieur Brillant, le rôle de l'intelligence artificielle en matière de crédibilisation des faux comptes. Dans le même temps, vous avez annoncé, Monsieur Strubel, que les moyens que vous espériez et qui vous ne seront pas accordés ne seront donc pas consacrés à l'intelligence artificielle. Dans la mesure où 30 % de vos moyens sont affectés aux Jeux olympiques et paralympiques depuis plusieurs années et où les moyens attendus ne seront pas débloqués cette année, à quoi allez-vous devoir renoncer ?

Lors de votre audition l'an passé, Monsieur le secrétaire général, vous aviez déclaré : « L'ANSSI va également lancer une révision de la stratégie de lutte contre les cyberattaques : celle-ci a été adoptée en 2018 et nous souhaitons la mettre à jour pour tenir compte des évolutions en matière de cybercriminalité ou de cyberattaques et en particulier de l'arrivée de l'intelligence artificielle et du quantique. Tout cela va complètement bouleverser la donne et nous amènera à revoir notre position, encore une fois, en liaison avec les autres ministères, pour jouer un rôle plus offensif ». Cette révision de la stratégie de lutte contre les cyberattaques a-t-elle pu être engagée ou est-elle remise en cause du fait de ces considérations budgétaires ?

Durant les évènements qui ont eu lieu au printemps en Nouvelle-Calédonie, la décision d'y suspendre le réseau social TikTok – qui n'est pas

anodine – a été prise, ce qui a suscité quelques interrogations de la part du Conseil d'État. Avez-vous été consultés avant cette suspension ?

Lorsqu'il y a un peu plus d'un an, nous nous préoccupions du cas de TikTok avec, concomitamment, la commission d'enquête du Sénat sur les ingérences étrangères et certaines décisions des institutions de l'Union européenne, la Première ministre a annoncé l'interdiction des applications récréatives sur un certain nombre de terminaux mobiles pour, notamment, les membres du Gouvernement et certains fonctionnaires. Cette interdiction est-elle opérationnelle ?

M. Stéphane Bouillon. – Sur l'interdiction des applications récréatives pour les communications à l'intérieur du Gouvernement, la messagerie Signal a remplacé les autres messageries utilisées auparavant.

Nous avons un temps mis à disposition des téléphones sécurisés, dits Mobius, avec des moyens extrêmement réduits puisqu'ils ne permettaient pas l'accès à internet, mais uniquement la téléphonie et les échanges de courriels. Ces téléphones, dont l'honnêteté m'oblige à dire qu'ils n'étaient pas très utilisés, ont été récupérés après le départ du dernier Gouvernement et nous allons les conserver cette année pour réaliser des économies.

Les ministres peuvent utiliser leur téléphone personnel pour un certain nombre d'activités, et notamment pour communiquer avec vous, le cas échéant, mais, à l'intérieur du Gouvernement, le Président de la République et le Premier ministre ont émis des instructions conjointes pour demander une réelle discipline et l'utilisation de Signal pour les échanges entre les membres du Gouvernement, leurs cabinets et les directions d'administrations centrales.

Nous n'avons pas été consultés en amont de la suspension de TikTok au printemps. Cette décision a été prise pour des motifs d'ordre public et l'a donc été assez rapidement. Nous en avons évidemment été immédiatement informés.

La stratégie de lutte contre les cyberattaques a été mise au point en interministériel. Il faut désormais que nous la fassions remonter vers le Président de la République et le Premier ministre pour l'approuver, la modifier ou l'encadrer. La situation budgétaire de cette année va bien sûr nous conduire à nous interroger sur un certain nombre de sujets. Il n'en reste pas moins qu'au travers de cette stratégie, toute une série d'actions concernant l'organisation, la gouvernance et d'autres domaines pourra être mise en œuvre. Un certain nombre d'investissements devront toutefois être décalés, notamment lorsqu'il s'agit d'investissements de sécurité, de redondance ou de multiplication de centres à différents endroits.

Je vais laisser Vincent Strubel réagir sur l'écart entre ce sur quoi nous essayons de travailler en matière d'intelligence artificielle et les moyens que nous allons pouvoir y consacrer. Je peux simplement dire que le sujet de l'intelligence artificielle ne peut pas être traité par la seule ANSSI, mais doit être travaillé avec tous les ministères concernés – et tous vont l'être. Il s'agira

d'un travail de long terme qui associera nos partenaires privés. En effet, nous devons rester humbles. La France a dû consacrer, je crois, 7 milliards d'euros à l'intelligence artificielle en quelques années. C'est une somme importante, mais Google y a dédié plusieurs centaines de milliards de dollars. De ce point de vue, il faut reconnaître que nous n'avons pas été capables d'organiser un groupe d'ampleur européenne en matière d'intelligence artificielle.

Concernant le *name and shame*, la question est traitée par le Comité de lutte contre les manipulations de l'information (Colmi) ou, pour ce qui concerne l'ANSSI, par le Centre de coordination des crises cyber (C4). Nous proposons toute une série de réponses, qui vont de l'attribution – si nous savons avec certitude de quel État il s'agit – à l'imputation – auquel cas nous expliquons que l'attaque a utilisé des modes d'action qui sont habituellement utilisés par des services chinois ou russes, par exemple, sachant que quelques États peuvent aussi se servir de ces modèles pour se cacher derrière une imputation autre. Nous faisons ensuite remonter l'affaire aux cabinets ministériels, puis au Président de la République et au Premier ministre, après quoi nous attendons des instructions.

Dans le cadre du jeu des relations internationales, avec, potentiellement, des visites de chefs d'État ou de gouvernement ou des conférences internationales à venir, il est intéressant de pouvoir se coordonner avec nos voisins européens pour pouvoir frapper plus lourdement. Le choix du calendrier dépend alors de considérations de politique intérieure ou étrangère et relève donc de l'autorité politique. En tout cas, le rapport que nous devons vous transmettre à la fin de l'année sur les actions que nous avons pu mener constitue un point d'arrivée qui permettra de mettre à jour toute la vérité.

Nous savons aussi travailler avec nos interlocuteurs de la presse et sommes capables de faire du off pour permettre à un média de signaler qu'une attaque a eu lieu. J'avoue d'ailleurs avec regret que l'information est parfois plus crédible quand elle provient d'un grand journal plutôt que d'un communiqué de presse, même si celui-ci émane du SGDSN.

Concernant les ajustements du périmètre d'action de l'ANSSI, nous avons souvent parlé avec Vincent Strubel de la place d'un opérateur au sein du SGDSN et donc auprès du Premier ministre, qui est plutôt un coordinateur et ne devrait pas disposer de services opérationnels. En réalité, les sujets de manipulation de l'information et les sujets cyber sont par nature interministériels : tout le monde est concerné et chaque ministère est compétent. Je ne suis pas sûr qu'à l'étranger, et en Allemagne en particulier, le débat autour de l'identité du ministère le mieux à même de suivre ces questions soit tranché, ce qui peut nuire à l'efficacité de l'action publique. Ma réponse est qu'il est important que le Premier ministre puisse disposer d'un outil sur ces sujets.

Cet instrument permet également au Premier ministre de vérifier que ses ministres assument leurs responsabilités en matière de cybersécurité au sein de leurs services. Tous les ans, une réunion a lieu entre le Premier ministre et les membres du Gouvernement ou entre leurs directeurs de cabinet pour établir le tableau d'honneur de ceux qui ont investi ou fait ce qu'ils devaient faire et le tableau d'horreur de ceux qui doivent encore mieux faire. Cette mission doit donc revenir au Premier ministre.

La régulation couvre toute une série de compétences, judiciaires, administratives ou financières. J'ai donc tendance là aussi à considérer qu'elle doit pouvoir demeurer à notre niveau.

Enfin, pour ce qui concerne la coordination avec les collectivités territoriales, il me paraît nécessaire que nous restions en charge, car il ne serait pas aisé autrement de déterminer si la responsabilité doit revenir au ministre de l'intérieur, à la ministre en charge des collectivités territoriales, au ministre de l'économie et des finances ou à la ministre en charge de la communication.

Chacun reconnaît l'aspect interministériel de notre mode de fonctionnement, y compris parce que nous organisons les conseils de défense, où tout le monde se retrouve sous l'autorité du SGDSN pour préparer un bilan de ce que nous faisons sur tel ou tel thème de sécurité – et des conseils sont régulièrement consacrés au cyber et à la lutte contre la manipulation de l'information – et pour proposer au Président de la République et au Premier ministre des orientations et des actions à mener.

J'ai la faiblesse de penser qu'il n'y pas de querelle de chapelle ou de compétence parce que nous essayons de bien faire notre travail. Tout le monde travaille efficacement et collectivement pour proposer des mesures qui seront admises par les décideurs et qui, par conséquent, passent facilement en conseil de défense.

M. Vincent Strubel. – Je souhaiterais partager avec vous ma conviction profonde, ancrée dans vingt années de parcours au sein de la cybersécurité : notre efficacité – le fait que nous arrivions à faire aussi bien que d'autres avec des moyens trois fois moindres – tient en grande partie à un modèle très intégré, avec une ANSSI placée sous l'autorité du SGDSN et, à travers lui, du Premier ministre, au-dessus de la mêlée interministérielle, qui intervient dans tous les champs et se porte garante de la cohérence des réponses de toute nature à la cybermenace.

L'ANSSI dispose en outre d'une force énorme, dans la mesure où les agents qui élaborent le cadre réglementaire, coordonnent les travaux européens ou font de la certification de produits ou de services travaillent main dans la main avec leurs collègues qui, au quotidien, regardent dans le blanc des yeux les meilleurs attaquants du monde et trouvent des réponses efficaces face à leurs attaques. Il en résulte que nous sommes écoutés – notre crédibilité est aussi l'une de nos forces – et que notre action est efficace face à la menace.

Ce modèle très intégré n'exclut pas la sous-traitance. Elle nous permet aujourd'hui de travailler avec un effectif réduit par rapport à nos voisins. Nous avons su déléguer une part énorme du traitement d'incidents au secteur privé ainsi qu'à de nouveaux acteurs, comme les CSIRT sectoriels ou régionaux. Pour autant, nous demeurons le chef d'orchestre ou la tour de contrôle, ancrés dans la réalité de la menace.

Par ailleurs, le *name and shame* n'est pas notre seul levier. Dénoncer publiquement constitue la réponse naturelle à une manipulation de l'information, parce qu'il s'agit de rétablir la vérité. Néanmoins, dans le domaine cyber, dire que tel ou tel pays nous attaque n'est pas forcément très dissuasif, car souvent de notoriété publique. Nous partageons donc quasi quotidiennement de l'information technique, quel que soit l'attaquant, sur les outils utilisés, les adresses IP ou les manières de repérer les attaquants qui mènent une campagne, et ce par le biais de mémos diffusés soit au sein de la communauté des sachants du cyber, soit publiquement, sur le site internet de l'ANSSI. Cette pratique permet de réduire les capacités de l'attaquant en les rendant détectables.

L'arbitrage est assez subtil, de même qu'en ce qui concerne le démantèlement d'infrastructures techniques d'attaquants, auquel nous recourons de plus en plus, en lien avec nos principaux alliés. L'opération End Game, menée sous pilotage américain avec la contribution de la France, de l'Allemagne et d'un certain nombre d'autres partenaires, consiste par exemple à détruire des infrastructures de l'attaquant. Le choix de recourir à ce procédé est toujours mûrement réfléchi car une fois ses infrastructures détruites, l'attaquant va revenir ailleurs et nous allons perdre le bénéfice de savoir où il se trouvait. En revanche, cette pratique présente une certaine utilité pour faire baisser la pression. Nous pouvons ainsi nous féliciter d'y avoir recouru contre certains attaquants avant les Jeux olympiques.

L'un des objectifs de la revue stratégique de cyberdéfense est d'ailleurs l'élaboration d'un inventaire des différents leviers dont nous disposons, la consolidation de notre algorithme d'utilisation de tel ou tel levier, si j'ose dire, et la détermination des niveaux de validation nécessaires.

Enfin, je tiens à vous dire que nous ne sommes pas désarmés face à l'intelligence artificielle. Nous entendons des discours très anxiogènes à ce sujet, qui donnent à penser que l'intelligence artificielle va révolutionner les pouvoirs des attaquants et que nous sommes totalement incapables d'apporter des garanties de sécurité dans ce domaine. Ça n'est pas vrai. L'ANSSI a publié cette année des lignes directrices et des recommandations sur la mise en œuvre sécurisée de l'intelligence artificielle générative. Nous en avons publié d'autres très récemment avec nos amis de l'Office fédéral de la sécurité des technologies de l'information (BSI) allemand sur la génération de codes logiciels avec l'intelligence artificielle.

Pour autant, nous sommes conscients des limites de nos connaissances ou de nos modèles. Un travail important reste donc à mener sur la transposition ou nos dispositions de certification à l'intelligence artificielle, par exemple, ce qui nécessitera un investissement conséquent. Même si nous n'allons pas renoncer au traitement de l'intelligence artificielle, le projet de création d'un laboratoire dédié à ces questions au sein de l'ANSSI devra être reporté à plus tard compte tenu du contexte budgétaire, sans que nous soyons pour autant totalement désarmés sur ce sujet.

Mme Hélène Conway-Mouret. – Vous avez très justement rappelé que la menace croissait et que vous avez été en capacité d'accompagner de nombreux acteurs pendant les Jeux olympiques. Nous auditionnons avec mon co-rapporteur de nombreux industriels, et notamment ceux qui sont liés à l'industrie de défense, dont les innovations sont très sensibles. Il en ressort que beaucoup de PME et d'ETI n'ont pas les moyens de se défendre contre le piratage, qui va du chantage au racket pour la récupération de leurs données. Comment, dès lors, protéger nos PME, qui sont vitales à notre industrie de défense ?

M. Ludovic Haye. – Je me joins aux félicitations de mes collègues concernant les Jeux olympiques. Votre succès démontre que l'on peut agir sur de tels dossiers lorsque l'on s'en donne les moyens. En l'occurrence, la coordination entre vos trois organismes a fait la preuve de son efficacité.

Si nous avons manqué le train des Gafam et du début de l'intelligence artificielle générative, le sujet est peut-être aujourd'hui de s'intéresser à l'utilisation des données synthétiques produites par l'intelligence artificielle. Le code du stockage souverain reste très important à mes yeux.

Le général Watin-Augouard me disait hier encore que, dès qu'un projet est lancé en France, il demande ce qu'il en est de son volet cyber. Je le rejoins sur ce point. Alors que nous parlons beaucoup de privacy by design et de security by design, vos structures sont-elles correctement organisées pour répondre à ce besoin d'anticipation ? En effet, en période de restrictions budgétaires, le préventif a tendance à s'effacer devant le curatif…

M. Jean-Marc Vayssouze-Faure. – Je souhaiterais que vous puissiez revenir sur la capacité des collectivités territoriales à se protéger.

J'ai relevé que l'ANSSI avait constaté, entre janvier 2002 et juin 2023, 187 incidents cyber concernant 131 communes et établissements publics de coopération intercommunale (EPCI), 42 départements, 12 régions et 2 collectivités d'outre-mer et que le projet de loi transposant la directive européenne NIS 2 avait bien intégré la question des collectivités locales, alors que l'appréciation en était soumise à chaque État membre.

Comment ces collectivités peuvent-elles se protéger aujourd'hui, sachant qu'elles risquent de subir des coupes budgétaires alors qu'elles devront certainement s'engager dans des investissements importants et

difficilement finançables et que, dans la plupart des cas, les petites communes ne disposent pas d'un responsable de la sécurité des systèmes d'information ?

Mme Gisèle Jourda. – Vous avez indiqué que le niveau urgence attentat avait été maintenu conformément à la volonté du Premier ministre. Nous avons été victimes, à Carcassonne et à Trèbes, d'un attentat qui a conduit au décès du colonel Beltrame.

Je souhaiterais savoir comment est maintenue la surveillance des personnes, qu'elles soient fichées S ou non, et comment est assurée la couverture de l'ensemble du territoire national, car nous n'aurions jamais imaginé être frappés dans des villes de cette importance.

On oublie bien souvent que, par-delà tous les moyens de surveillance et de protection face aux cyberattaques dont nous disposons, certains reviennent à des moyens beaucoup plus traditionnels. Il ne faut pas qu'ils passent à travers les mailles du filet.

M. Philippe Folliot. – Je m'associe aux propos qui ont été tenus par mes différents collègues pour vous féliciter collectivement pour l'excellence de votre travail à l'occasion des Jeux olympiques. En effet, les regards du monde entier étaient braqués sur nous et nous n'avions pas droit à l'erreur.

Au rugby, on dit souvent que l'attaque – ou la contre-attaque – est la meilleure des défenses. De quels moyens disposons-nous pour faire face à cette guerre informationnelle entre le bloc des démocraties d'un côté et le bloc des dictatures ou des régimes autoritaires de l'autre ?

Nous avons été particulièrement choqués de l'action de l'Azerbaïdjan lors des évènements du printemps dernier en Nouvelle-Calédonie. Ne disposons-nous pas d'éléments pour contre-attaquer et révéler un certain nombre de choses sur la situation réelle de ces régimes ?

M. Stéphane Bouillon. – Je reviendrai en premier lieu sur les sujets de sécurité économique et la protection des PME et des ETI pour la récupération des données.

Nous travaillons beaucoup avec le ministère de l'économie et des finances et l'ensemble des responsables de l'industrie de défense pour faire en sorte d'améliorer le niveau de connaissance de ces enjeux et nous nous appuyons sur les préfets dans les départements et les régions pour qu'ils restent vigilants concernant ce qui peut se passer dans les PME.

Vincent Strubel a l'habitude de dire que, quand un lion vous court après dans la jungle, l'enjeu n'est pas de courir plus vite que le lion, mais de courir plus vite que votre voisin. Il convient donc de disposer d'une protection qui permet d'échapper à une attaque. En outre, la cybersécurité d'une entreprise peut être assurée en y consacrant un investissement de l'ordre de 10 % du budget cyber de l'entreprise.

S'agissant des collectivités locales, j'ai eu l'occasion de dire au président d'Intercommunalités de France qu'il fallait essayer de travailler sur ces sujets au niveau intercommunal. Il serait illusoire de le faire dans une petite commune.

D'autre part, comme je l'ai évoqué avec le Gouvernement précédent et réévoqué avec le nouveau, je pense qu'il faudrait permettre à l'État de subventionner les collectivités au travers des dotations de soutien aux investissements, et notamment la dotation d'équipement des territoires ruraux (DETR) et la dotation de soutien à l'investissement local (DSIL), de la même manière que leurs investissements informatiques ont été subventionnés par le passé.

Concernant le risque d'attentat, les services de renseignement surveillent de très près ce qui se passe sur les réseaux sociaux. Les trois attentats qui ont été évités en début d'année l'ont été parce que leurs auteurs annonçaient sur les réseaux sociaux qu'ils allaient passer à l'acte.

Pour répondre à la question relative à la défense et à l'attaque, je dirais que nous sommes tous les trois des pompiers. Nous essayons de prévenir les attaques et nous protégeons d'elles. Nous ne sommes donc pas à l'offensive et ne souhaitons pas l'être. Si nous l'étions, nous perdrions sans doute beaucoup de notre crédibilité ou la confiance des médias, des acteurs et des opérateurs. Imaginez que l'ANSSI puisse conduire une attaque en matière cyber ; je ne suis pas certain que toutes les collectivités s'adresseraient spontanément à elle. Imaginez également que l'Agence puisse aspirer les données des acteurs qu'elle vient sauver ; plus personne ne ferait appel à elle, ce qui serait désastreux pour les entreprises. Nous tenons donc à conserver notre rôle dans ce domaine.

La difficulté en matière de manipulation de l'information est qu'il s'agit d'une menace totalement asymétrique. Nous sommes des démocraties. Essayer de faire de la manipulation de l'information en Chine, en Russie ou dans d'autres pays est absolument illusoire, d'abord parce qu'il n'y a pas de liberté de l'information et ensuite parce que le premier qui commencera se fera évidemment bloquer immédiatement.

Dans cette situation asymétrique, le *name and shame* est important non seulement pour porter atteinte à la réputation de ces pays – et certains y sont sensibles –, mais aussi pour permettre à l'ensemble de nos concitoyens de comprendre que telle information a été fabriquée non pas à Paris, à Marseille ou à Carpentras, mais à Pékin, à Saint-Pétersbourg ou à Ankara. En général, les pays concernés n'apprécient pas et se dépêchent de démentir, ce qui prouve que nous avons une certaine efficacité sur ce sujet.

Enfin, pour ce qui concerne les sujets de stockage souverain, l'enjeu, aujourd'hui, est précisément d'aider l'ensemble des acteurs à s'organiser, à prévenir et à intégrer les sujets de cybersécurité le plus tôt possible.

Pour terminer sur une note optimiste, je tiens à rappeler que, bien que la France soit en retard sur l'intelligence artificielle, nous sommes bons, voire très bons, sur le quantique. Les appels téléphoniques qui me venaient de la National Security Agency (NSA) des États-Unis pour me dire leur souhait de travailler avec nous en quantique me conduisent à penser que nous avons de l'avance. Il nous appartient de travailler sur ce sujet pour continuer à progresser.

M. Cédric Perrin, président. – Merci beaucoup pour le temps que vous nous avez consacré. Nous ne doutons pas que malgré la contrainte budgétaire, vous allez faire face avec toujours autant de brio. Vous pouvez en tout état de cause compter sur cette commission pour veiller au vote et à la bonne exécution du budget.

Nous traversons une période où chacun fait des efforts et où tous les services de l'État sont mis à contribution. Il est quelque peu surprenant de constater que les questions d'influence, d'ingérence et de défense face à ce nouveau type d'attaques en font les frais, mais c'est ainsi. À vous d'être bons avec des moyens qui ne sont pas forcément à la hauteur de nos ambitions.

Nous restons bien entendu à votre disposition pour vous aider, vous accompagner et continuer à porter ces sujets qui sont peut-être parfois mal compris du grand public, mais qui correspondent à une nouvelle forme de guerre commencée depuis un certain temps déjà et à laquelle nous sommes confrontés quotidiennement. Je ne pense pas, du reste, que les évènements de cette nuit aux États-Unis amélioreront la situation.

LISTE DES VISITES ET DES PERSONNES ENTENDUES

Mardi 15 octobre 2024 :

- MM. Cédric Mora, Policy Manager de AWS et Arnaud David, Director of Public Policy d'AWS
- Général de corps d'armée Hervé de Courrèges, directeur de l'IHEDN

Mercredi 16 octobre 2024 :

- Visite du GIP ACYMA Cybermalveillance en présence de MM. Jérôme Notin, directeur général

Mardi 29 octobre 2024 :

- Visite de Viginum (Vigilance et protection contre les ingérences numériques étrangères), en présence de M. Marc-Antoine Brillant, chef du service

Mercredi 30 octobre 2024 :

- M. Patrick Guyonneau, Directeur de la Sécurité du Groupe Orange, et Carole Gay, Responsable des relations institutionnelles à la Direction des Affaires Publiques du Groupe Orange
- Monsieur Kim Nguyen, Vice-président Systèmes d'information numérique, Université Paris-Saclay

Jeudi 31 octobre 2024 :

- M. Daniel Le Coguic, en qualité de vice-président Cyber d'ATOS
- Table ronde avec MM. Daniel Le Coguic, en qualité de président de l'ACN, Yoann Kassianides, délégué général, Mme Elsa Auriol, responsable des affaires publiques de l'ACN, MM. Antonin Hily, CEO de Sesame it, et Antoine Berthault-Barrenechea, directeur de clientèle de Rumeur Publique
- Raphaël Beaufret, Directeur des services numériques de l'AH-HP

Mardi 5 novembre 2024 :

- Visite du centre opérationnel de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en présence de M. Vincent Strubel, directeur général.

Mercredi 6 novembre 2024, en audition plénière :

- Stéphane Bouillon, secrétaire général du SGDSN, Vincent Strubel, directeur général de l'ANSSI et de Marc-Antoine Brillant, chef du Service de vigilance et de protection contre les ingérences numériques étrangères (Viginum)