…l'avis de la commission sur le projet de loi de finances pour 2024

RÉORGANISER LA COORDINATION DES POLITIQUES DE CYBERSÉCURITÉ ET DE LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION

Rapport pour avis n° 130 tome IX (2023-2024) de MM. Olivier CADIC et Mickaël VALLET sur les crédits de l'action n° 2 « Coordination de la sécurité et de la défense » du programme 129 « Coordination du travail gouvernemental » de la mission « Direction de l'action du Gouvernement ».

La cybersécurité et la lutte contre les manipulations de l'information correspondent à une partie des missions du Secrétariat général de la défense et de la sécurité nationale (SGDSN) dont le financement relève de l'action n°2 « coordination de la sécurité et de la défense »[1]. L'exercice 2024 se caractérise par un **renforcement des moyens de l'agence nationale de la sécurité des systèmes d'information (ANSSI) et du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum)**, constituant ainsi le volet civil de l'effort prévu par la loi de programmation militaire 2024-2030 (4 milliards d'€ de besoins programmés sur la période)[2].

Pour répondre au « **changement d'échelle** » annoncé par l'ANSSI qui est de passer à une cybersécurité de masse, vos rapporteurs ont identifiés **4 principaux défis à relever** :

- **assurer la cybersécurité des Jeux olympiques et paralympiques 2024**. Pour l'image internationale de la France, il n'y aura pas de médaille d'argent ;

- **coordonner** l'ensemble des acteurs publics et privés de l'écosystème cyber autour d'une **révision de la stratégie nationale de cybersécurité** (la dernière datant de 2018) et du lancement de la **plateforme numérique « 17 Cyber »** en mars 2024 ;

- **réussir la transformation de l'ANSSI en vue de la transposition de la directive NIS 2** (Network and Information Security[3]). 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 ;

- **réorganiser le dispositif de coordination** en s'inspirant de la grande cause nationale de la sécurité routière qui a permis de réduire drastiquement le nombre de morts sur nos routes en confiant à **un coordinateur interministériel clairement identifié** la responsabilité de coordonner tous les moyens disponibles.

[1] Compte tenu de la dimension transversale de la coordination de ces politiques publiques par les services de la Première ministre, en lien avec certaines unités et services relevant de la mission « Défense » - commandement de la cyberdéfense, direction générale de la sécurité extérieure – un suivi en est assuré par la commission des affaires étrangères et de la défense.

[2] Le taux de réponse au questionnaire budgétaire est de 100 %, l'ensemble des réponses aux 44 questions adressées au Gouvernement, avant le 10 juillet 2023, ayant obtenu une réponse dans le délai fixé par l'article 49 de la loi organique n° 2001-692 du 1er août 2001 relative aux lois de finances, à savoir au plus tard le 10 octobre suivant.

[3] Sécurité des réseaux et de l'information.

1. LES CHIFFRES CLÉS DE L'ACTION N°2 « COORDINATION DE LA SÉCURITÉ ET DE LA DÉFENSE » CONTRE LES MENACES CYBER ET HYBRIDES

A. LE PANORAMA DES MENACES : UNE INDUSTRIALISATION DE LA CYBERCRIMINALITÉ ET DES MANIPULATIONS DE L'INFORMATION

Avec **831 intrusions avérées**[1] **répertoriées par l'ANSSI en 2022**, contre 1 082 en 2021, le niveau de la cybermenace marque **une pause en trompe l'œil**. D'une part, **la gravité des attaques s'est accentuée**, rendant nécessaire **19 opérations de cyberdéfense dont 9 d'entre-elles ont caractérisé des modes opératoires affiliés à la Chine**. D'autre part, la pression cybercriminelle demeure élevée avec un regain d'événements traités par l'ANSSI en **hausse de 23 % au premier semestre 2023** par rapport à 2022, dont **50 % d'augmentation des extorsions de fonds** sous forme de « rançongiciel ».

Signe de la montée en compétence et de l'industrialisation des attaques contre la sécurité des systèmes d'information de l'Etat, l'ANSSI a été saisi de **227 incidents cyber affectant des ministères**, contre 222 en 2021 et 128 en 2020. Le tableau ci-dessous présente la répartition entre ministères des incidents et leur niveau de gravité.

Tableau des cyber incidents par ministère traités par l'ANSSI

Ministères	Nombre d'incidents traités par l'ANSSI				Caractérisation des incidents
	2019	2020	2021	2022	
Ministère de l'agriculture et de l'alimentation	8	14	3	2	
Ministère de la cohésion des territoires	0	2	2	0	
Ministère de la culture	6	11	10	6	Dont un incident notable
Ministère des armées	22	4	5	2	Dont deux incidents notables
Ministère de l'économie des finances et de la relance	11	18	24	8	Dont un incident notable
Ministère de l'éducation nationale, de la jeunesse et des sports	22	58	149	187	Dont 181 compromissions de comptes de messagerie
Ministère de l'enseignement supérieur, de la recherche et de l'innovation	1	3	0	0	
Ministère de l'Europe et des affaires étrangères	14	14	10	5	Dont 1 opération de cyberdéfense et un incident notable
Ministère de l'intérieur *et des outre mer**	14	13	11	4	
Ministère de la justice	6	4	4	2	Dont une opération de cyberdéfense
Ministère des outre-mer	1	2	*	*	* regroupé avec le chiffrage du ministère de l'intérieur
Ministère de la santé et des préventions	3	14	6	6	
Ministère de la transition écologique	8	18	12	6	
Ministère du travail, de l'emploi et de l'insertion	7	6	1	0	

Source : réponse au questionnaire budgétaire

[11] Panorama de la cybermenace 2022 (ANSSI).

Ce tableau qui ne recense que les actions directement menées par l'ANSSI doit être complété par plusieurs indicateurs :

- **Dans le ressort des armées**, au lieu de 150 événements traités par le commandement de la cyberdéfense (COMCYBER) en 2021, on enregistre **une baisse de 50 % de ce nombre en 2022 avec 75 événements** (8 incidents cyber et 67 alertes) dont les 2 mentionnés plus haut en collaboration avec l'ANSSI. À cet égard, le conflit ukrainien n'a semble-t-il pas engendré de ciblage particulier de la France ;

- S'agissant des particuliers, entreprises et collectivités territoriales (hors OIV et OSE[1] suivis par l'ANSSI), le GIP ACYMA en charge de **la plateforme cybermalveillance.gouv.fr a vu sa fréquentation augmenter de 53 % en 2022 avec 3,8 millions de visiteurs** (2,5 millions en 2021) et **280 000 demandes d'assistance** contre 170 000 en 2021. Les grandes tendances observées par la plateforme porte sur une progression de l'hameçonnage (*phishing*) lequel représente la première recherche d'assistance des particuliers (38 %), des collectivités territoriales et administrations (28 %) et des entreprises et associations (27 %). Suivent la violation des données (16 %), le piratage de compte (14 %) et les fausses offres de support technique (9 %) ;

- En matière de **lutte contre les manipulations de l'information** (LMI), un service de de vigilance et de protection contre les ingérences numériques étrangères (Viginum) a été créé à l'automne 2021 afin de détection et de caractérisation des ingérences numériques étrangères. Encore en phase de montée en puissance, ce service a détecté **78 phénomènes dits « potentiellement inauthentiques » en 2022 pour lesquels 7 d'entre eux ont été caractérisés comme des ingérences étrangères**. Dans le cadre de la présidentielles 2022, en lien avec le Conseil constitutionnel, le juge de l'élection, Viginum a également dénombré **cinq ingérences relevant du « phénomène BETH »** attribué à des opérations liées à la Russie (cf. encadré ci-dessous).

L'exemple de deux opérations de désinformation attribuées à la Russie

Viginum a détecté, caractérisé et rendu publiques deux opérations de manipulation de l'information qui ont pour trait commun leur attribution à la Russie :

- **en 2022, cinq cas d'ingérences numériques étrangères sur les élections présidentielles et législatives de 2022** ont été caractérisés, dont le « phénomène Beth » qui consiste en une opération de promotion d'un candidat par des « fermes à trolls », lesquelles sont à l'origine de la « diffusion artificielle ou automatisée, massive et délibérée », via de faux comptes de réseaux sociaux, de « contenus manifestement inexacts ou trompeurs » ;

- en 2023, c'est à partir d'un dossier établi par Viginum que le ministère de l'Europe et des affaires étrangères a communiqué sur une **campagne russe de manipulation de l'information**, dénommée RRN en raison de la place centrale occupée par le média *Reliable Recent News*, visant à diffuser des contenus pro-russes liés à la guerre en Ukraine et à discréditer les médias et gouvernements de plusieurs États européens, dont la France, par l'utilisation de faux comptes ou l'usurpation de site et d'identité[2].

B. LES MOYENS CYBER ET DE LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION DU SGDSN

En 2024, sur un total de 438,8 M€ en crédits de paiement dévolus à l'action n°2 « Coordination de la sécurité et de la défense, le SGDSN dispose de 315,8 M€ dont **132 M€ répartis entre les trois services à compétence nationale** chargés de la sécurité des systèmes d'information de l'État et de la lutte contre les manipulations de l'information.

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

[2] Source : https://www.sgdsn.gouv.fr/publications/maj-19062023-rrn-une-campagne-numerique-de-manipulation-de-linformation-complexe-et

Ce montant est en **augmentation de près de 15 % par rapport à la LFI 2023** (115 M€), dont un quasi doublement des effectifs de Viginum et une augmentation de 40 ETPT[1] de l'ANSSI et de 10 ETPT de l'OSIIC, notamment pour faire face à la préparation des Jeux olympiques 2024.

Évolution des moyens des trois opérateurs du SGDSN pour 2024

Agence nationale de la sécurité des systèmes d'information (ANSSI)
81,8 M€ en 2024
(+8,9 M€ par rapport à 2023)
644 ETPT en 2024
(+ 40 ETPT par rapport à 2023)

Opérateur des systèmes d'information interministériels classifiés (OSIIC)
44 M€ en 2024
(+6,2 M€ par rapport à 2023)
135 ETPT en 2024
(+10 ETPT par rapport à 2023)

Service de vigilance et de protection contre les ingérences numériques étrangères (Viginum)
6 M€ en 2024
(+1,6 M€ par rapport à 2023)
42 ETPT en 2024
(+17 ETPT par rapport à 2023)

Le cyber et la LMI ne représentent donc qu'une partie des missions du SGDSN, lequel répartit les quelques 184 M€ restant entre ses activités transverses de secrétariat du conseil de défense et de sécurité nationale, de prévention des crises et de coordination des politiques interministérielles de protection (72 M€), de financement des capacités techniques interministérielles (103 M€) et de subvention à l'Institut des hautes études de la défense nationale (7,8 M€).

C. DES MOYENS PARTICULIERS MIS À DISPOSITION DES SERVICES DE RENSEIGNEMENT :

Les autres crédits de l'action n°2 sont fléchés vers des dispositifs concourant aux missions des services de renseignement :

- **75,97 M€ pour le financement des fonds spéciaux** dont l'essentiel concerne principalement la DGSE, la ventilation exacte des crédits entre les services dits du « premier cercle » n'étant pas publiée car relevant du secret de la défense nationale. Un contrôle parlementaire de leur usage est toutefois effectué par la commission de vérification des fonds spéciaux (CVFS). Il convient de relever que ce montant prévisionnel (environ 76 M€) est inchangé depuis 2020. Mais du fait de l'actualité internationale et de l'évolution de l'activité des services, **on constate presque systématiquement, sauf en 2021, des dépassements dans l'exécution budgétaire** (+ 6M€ en 2020, + 25 M€ en 2022 et + 26 M€ au premier semestre 2023). **Si l'on considère que les services liés à la sécurité extérieure et intérieure de la Nation vont poursuivre leurs efforts en 2024** (guerre en Ukraine, reconfiguration des forces en Afrique, tensions en Indopacifique autour de la situation de Taïwan et résurgence d'une crise majeure au Proche et Moyen-Orient), 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 ;

- **47 M€ pour le fonctionnement du groupement interministériel de contrôle,** dont la mission est de centraliser les demandes d'autorisation de mise en œuvre des techniques de renseignement émises par les services. Ce montant, en hausse de 4,8 M€ par rapport à 2023 est justifié par l'augmentation de +2,2 % des demandes émises depuis 2022 par les services ainsi que par l'évolution des besoins en personnels, informatiques et immobiliers.

[1] Equivalent temps plein travaillé.

2. LES QUATRE PRINCIPAUX DÉFIS DE LA CYBERSÉCURITÉ EN 2024

Vos rapporteurs ont identifié au cours de leurs auditions **quatre principaux défis** à relever en 2024 pour atteindre l'objectif d'une « résilience cyber de premier plan » fixé par la revue nationale stratégique 2022 :

- **Assurer la cybersécurité des Jeux olympiques et paralympiques 2024**. Le pilotage en a été confié à l'ANSSI mais l'on note encore trop peu de collaborations avec les entreprises privées, sachant qu'il a été identifié qu'un effort particulier doit être orienté vers toute la chaîne des entreprises de sous-traitance ;

- **Coordonner l'ensemble des acteurs publics et privés** de l'écosystème cyber autour d'une **révision de la stratégie nationale de cybersécurité** (la dernière datant de 2018) et du **lancement de la plateforme numérique « 17 Cyber »** en mars 2024. Chaque ministère et chaque entité sont dotés d'un coordinateur : l'ANSSI qui est à la fois un régulateur et un acteur, le Secrétariat général pour l'investissement qui pilote le milliard d'euros de crédits de la stratégie nationale cyber[1], mais aussi Cybermalveillance pour les particuliers, TPE, PME, ETI et les collectivités territoriales, auxquels s'ajoute également le ministère de l'intérieur qui a pris la charge financière de la création de la future plateforme « 17 cyber ». Se pose la question de la stratégie de communication pour la diffusion de ce nouveau service au plus grand nombre : quel budget pour quels médias[2] ?

- **Réussir la transformation de l'ANSSI** en vue de la transposition de la directive NIS 2 (Network and Information Security). 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 et nécessite une reconfiguration de son offre de services ;

- **Réorganiser le dispositif de coordination** en s'inspirant de la grande cause nationale de la sécurité routière qui a permis de réduire drastiquement le nombre de morts sur nos routes en confiant à **un coordinateur interministériel clairement identifié** la responsabilité de coordonner tous les moyens disponibles.

Pour la cybersécurité des Jeux olympiques et paralympiques 2024, il n'y aura pas de médaille d'argent !

Concernant l'ANSSI, les constats et recommandations établis dans le cadre du rapport d'information[3] sur la préparation de la loi de programmation militaire 2024-2030 demeurent pleinement d'actualité pour :

- clarifier le périmètre de la transposition en France de la directive NIS 2 ;
- établir un plan de progression des moyens de l'ANSSI, de l'OSIIC et de Viginum en rapport avec l'augmentation du périmètre de protection de la directive NIS 2.

Plus largement, il ressort des auditions que la méthode de travail de **l'agence doit profondément évoluer pour s'adapter au « changement d'échelle »** qui va la conduire à animer non pas un réseau de quelques centaines de grandes entreprises mais de plusieurs

[1] Ce budget d'un montant de 1,1 milliard d'euros comprend une dotation de 176 millions d'euros pilotée par l'ANSSI dans le cadre du volet cybersécurité du Plan de relance.

[2] Les crédits consacrés à parité par la Gendarmerie et la Police nationale sont de 700 000 euros pour la première année de mise en œuvre, comprenant les coûts de développement, puis de 300 000 euros pour les années suivantes. À la date des auditions, les options de communication (comprises entre 300 000 euros et 2 millions d'euros) n'étaient pas encore arbitrées qu'il s'agisse d'une diffusion très grand public sur des médias nationaux ou d'une communication en ligne seulement sur internet.

[3] Rapport n° 638 (2023-2024)

milliers de PME et TPE. Selon le panorama de la cybermenace 2022, ce sont ces dernières qui sont la cible de 60 % des attaques :

- l'ANSSI est reconnue **comme un partenaire efficace et de confiance** par les OIV et OSE. En revanche, l'agence reconnait elle-même que **son offre de service n'est pas lisible** au-delà de ce cercle restreint ;
- la date d'entrée en vigueur de la directive NIS 2 est fixée au mois d'octobre 2024 mais il n'existe à ce stade **ni périmètre des entités concernées, ni document qui regroupe les exigences réglementaires** qui leur seront applicables ;
- l'animation d'un réseau de collectivités territoriales et d'entreprises autres que les OIV et les OSE est manifestement un métier nouveau pour l'ANSSI et, tant les grands opérateurs que les collectivités territoriales, s'inquiètent de **l'absence d'une feuille de route sur le calendrier et les étapes de discussion** pour la mise en œuvre de la directive NIS 2 ;
- **plusieurs autres points d'attention** ont été soulevés quant à la nécessité d'adapter la politique de labellisation de l'ANSSI aux besoins des TPE et PME, d'éviter toute sur-transposition de la directive qui créerait une distorsion de concurrence entre les entreprises françaises et européennes, enfin de revoir les secteurs où l'agence est à la fois l'organe de régulation et un acteur du marché (sondes EDR[1], centre de réponse aux incidents cyber, etc.).

Enfin, le même constat relatif à l'**absence de pérennité du financement des centres cyber régionaux**, lequel n'est pas assuré au-delà de l'amorçage du Plan de relance, justifie que les régions signalent le risque de devoir assumer seule la charge d'une mission régalienne.

POUR EN SAVOIR +

- **Compte rendu de l'audition de M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale (SGDSN), du général de brigade aérienne Emmanuel Naëgelen, directeur adjoint de l'Agence nationale de sécurité des systèmes d'information (ANSSI) et de M. Marc-Antoine Brillant, chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum)**

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

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

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

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

Mickaël Vallet
Rapporteur
Sénateur de la Charente-Maritime (SER)

[1] Endpoint Detection and Response : sonde de détection et de réponse pour les terminaux.