N° 130

SÉNAT

SESSION ORDINAIRE DE 2023-2024

Enregistré à la Présidence du Sénat le 23 novembre 2023

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 adopté par l'Assemblée nationale en application de l'article 49, alinéa 3, de la Constitution, pour* **2024**,

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. Jean-Noël Guérini, 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, Mme Gisèle Jourda, 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 (**16**ème législ.) : **1680**, **1715**, **1719**, **1723**, **1745**, **1778**, **1781**, **1805**, **1808**, **1820** et T.A. **178**

Sénat : **127** et **128** à **134** (2023-2024)

SOMMAIRE

Pages

L'ESSENTIEL

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.*

I. 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

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

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

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).

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

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[1].

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. 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[2] 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)

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

[2] *Equivalent temps plein travaillé.*

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.

II. 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 !

[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.

Concernant l'ANSSI, les constats et recommandations établis dans le cadre du rapport d'information[1] 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 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[2], 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.

---

[1] *Rapport n° 638 (2023-2024)*

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

EXAMEN EN COMMISSION

I. EXAMEN DU RAPPORT (15 NOVEMBRE 2023)

Au cours de sa réunion du mercredi 15 novembre 2023, la commission des affaires étrangères, de la défense et des forces armées, sous la présidence de M. Philippe Paul, vice-président, a procédé à l'examen du rapport de MM. Olivier Cadic et Mickaël Vallet, sur les crédits de la coordination du travail gouvernemental (action 2 Coordination de la sécurité et de la défense, SGDSN, Cyberdéfense).

M. Mickaël Vallet, rapporteur - Les crédits du programme 129 que nous vous présentons chaque année, avec mon collègue Olivier Cadic, portent sur l'action relative à la coordination de la sécurité et de la défense, et plus précisément sur la cybersécurité et la lutte contre les manipulations de l'information.

Vous avez été destinataires des chiffres clés de la menace cyber et des principaux défis à relever pour 2024. Aussi, passerons-nous plus rapidement sur ces éléments pour nous concentrer sur nos principaux constats et recommandations.

Quelques mots sont nécessaires pour décrire l'industrialisation de la cybercriminalité et des manipulations de l'information.

Avec 831 intrusions avérées répertoriées par l'ANSSI en 2022, contre 1 082 en 2021, le niveau de la cybermenace semble marquer une pause. Mais comme nous l'a rappelé le Secrétaire général de la défense et de la sécurité nationale que nous avons entendu en audition, il s'agit d'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 ». S'agissant des particuliers, entreprises et collectivités territoriales (hors opérateurs d'importance vitale et opérateurs de services essentiels 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. On peut certainement remarquer que la cybermenace évolue, mais aussi que ce phénomène est maintenant mieux connu de la population.

Vous avez certainement tous observé dans vos circonscriptions des attaques sur les collectivités territoriales, les hôpitaux et le tissu des PME et TPE. L'objectif de « résilience cyber » défini par la revue nationale

stratégique de 2022 prévoit une plus grande mutualisation des bonnes pratiques entre le public et le privé. Cela ne peut pas être que vertical. C'est tout un écosystème de cybersécurité qu'il convient de construire. C'est bien de le dire, et le Président de la République a clairement affiché des objectifs lors de son discours de Nice en janvier 2022 sur la sécurité. J'en rappelle ici les principaux volets. Il a annoncé, je cite : « un plan d'investissement technologique mais également de formation et de recrutement sans précédent au sein des forces de sécurité intérieure pour aller chercher les meilleurs profils issus de la société civile ». Ce plan comprend plusieurs dispositifs :

- la création d'une école de formation cyber au sein du ministère de l'intérieur pour former les policiers, les gendarmes et les agents des services de renseignement ;

- la mise en place d'un équivalent numérique de « l'appel 17 » afin que chaque citoyen puisse signaler en direct une attaque cyber et être mis immédiatement en relation avec un opérateur spécialisé. Au lieu d'un numéro de téléphone, il s'agit plutôt d'un signalement numérique ;

- la mobilisation des services de police et de gendarmerie dans les territoires pour sensibiliser les français, les entreprises, les collectivités à la menace cyber ;

- enfin, le déploiement massif d'un milliard d'euros d'investissements pour être plus performant dans la lutte contre ce nouveau risque.

C'est bien de le dire, maintenant il faut le faire et nous comprenons tous que ce sujet de coordination ne peut pas se limiter au cercle restreint des services de la Première ministre, SGDSN et ANSSI, mais qu'il faut réunir autour d'un même objectif tous les ministères et services concernés.

Je passe la parole à mon collègue sur les défis à relever en 2024, la question des moyens mis en œuvre et la nécessaire coordination de l'ensemble.

M. Olivier Cadic, **rapporteur –** Après consultation de personnalités de la sphère publique comme du secteur privé, nous voyons quatre défis principaux pour le cyber en 2024. D'abord, assurer la cybersécurité des Jeux olympiques et paralympiques 2024 pour une question d'image internationale. Il n'y aura pas de deuxième place. Ensuite, 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 en mars 2024 de la plateforme numérique « 17 Cyber » ouverte au grand public. Enfin, 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 pour l'agence et nécessite une reconfiguration de son offre de services.

A ces trois défis s'ajoute un quatrième défi que nous avions développé dans notre rapport préparatoire à la LPM et qui concerne l'organisation, ou plutôt la réorganisation du dispositif de coordination pour répondre au « changement d'échelle » annoncé par l'ANSSI qui est de passer à une cybersécurité de masse.

Cette nécessité de refonte de la stratégie résulte des nombreux points d'attention que les services et entreprises que nous avons auditionnées ont soulevés, à commencer par un brouillard quant à l'organisation de la réponse aux incidents cyber entre l'ANSSI responsable des systèmes de l'État et des opérateurs d'importance vitale, la plateforme cybermalveillance responsable de tout le reste mais sans les moyens associés, et l'amorçage par l'ANSSI de centres régionaux dont ni les services, ni le financement ne sont à ce jour garantis dans leur efficacité et leur pérennité. S'il y a une attaque, que se passe-t-il ? A qui s'adresse-t-on ? Il y a l'ANSSI qui suit les services de l'État et les OIV. Cybermalveillance est censé suivre tous les autres acteurs, mais il y a aussi des CERT sectoriel et des C-SIRT régionaux.

En réalité, chaque ministère et chaque entité s'est doté d'un coordinateur : l'ANSSI qui est à la fois un régulateur et un acteur, le Secrétariat général pour l'investissement dont nous avons rencontré ce matin le coordinateur, M. Florent Kirchner, mais aussi Cybermalveillance dont c'est le rôle d'être à la croisée de tous les chemins, et maintenant le ministère de l'intérieur qui a pris la charge financière de la création de la future plateforme « 17 cyber » en application des annonces du Président de la République.

Le fait que la menace cyber soit largement prise en compte va en soi dans le bon sens comme le rappelait le Directeur général de la gendarmerie nationale. En revanche, il nous semble qu'une chaîne claire de traitement et d'escalade des incidents soit définie. Il nous a été certifié que ce travail était en cours. Nous prenons date pour le lancement du « 17 cyber » prévu en mars 2024. Mais à quelques mois de ce rendez-vous important, il reste encore à définir les services offerts que cette plateforme numérique apportera à la population, et surtout comment la population sera informée de sa mise en service, selon quelle communication, avec quels crédits ?

Le message de l'ANSSI est de dire qu'il est encore trop tôt pour dessiner un « jardin à la française » et qu'il faut d'abord laisser l'écosystème public/privé de la cybersécurité se développer avant de tailler les haies. C'est une approche qui laisse certaines entreprises sur leur faim (Orange ou Thales) car elles ont besoin d'une feuille de route claire et d'y être associées notamment pour la transposition de la directive NIS 2 qui interviendra en octobre 2024.

Nous partageons ce besoin de clarification. Pour reprendre la métaphore du jardin à la française, il nous semble au contraire urgent de définir une organisation de coordination et de suivi de la qualité, bref de dessiner les allées du jardin dès maintenant, sinon le risque est de voir se développer une jungle ou tout le monde sera perdu. J'ajoute que l'enjeu de sécurité des Jeux Olympiques justifie l'urgence de la concertation, ce qui est un métier nouveau pour l'ANSSI.

C'est pourquoi, parmi nos propositions figurent celle d'actualiser la stratégie nationale de cybersécurité – l'actuelle date de 2018 – en y associant en amont tout l'écosystème sans oublier les collectivités locales, ni vos serviteurs.

Nous recommandons également de s'inspirer 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 unique la responsabilité de coordonner tous les moyens disponibles. Est-ce le rôle de l'ANSSI ou d'un délégué interministériel clairement identifié ? C'est à l'exécutif de le décider mais c'est à nous de signaler que l'année 2024 est le bon moment pour le faire.

Au bénéfice de ces observations, nous vous proposons l'adoption des crédits de la mission « Direction de l'action du Gouvernement ».

Mme Marie-Arlette Carlotti. **–** Je remercie nos collègues d'avoir décrit la menace cyber en la resituant dans un cadre plus large que les seuls services de l'État et des grandes entreprises. Ce sujet est particulièrement inquiétant et d'ailleurs le Sénat, ni les parlementaires ne sont à l'abri de ces attaques. Tous nos collègues sont informés par le biais de séances de sensibilisation organisées par les commissions mais il faut continuer.

M. Alain Joyandet. **–** C'est une grande cause et le politique doit reprendre la main sur les administrations centrales car ce problème touche aussi les collectivités territoriales et plus largement toute la population. Il s'agit d'un problème d'efficacité car pour assurer la sécurité du pays on ne peut pas se contenter d'empiler, comme vous l'avez dit, des dispositifs et de nouveaux coordonnateurs. Il faut réformer et simplifier.

M. Olivier Cadic – Il faut être réaliste. L'objectif n'est pas de supprimer les attaques. Il y en aura toujours et de plus en plus. On voit bien que les banques et les institutions sont ciblées par des attaques visant à saturer leurs systèmes et à engendrer des dénis de services. Le vrai sujet est celui de la résilience, c'est-à-dire la capacité à protéger mais aussi relancer les systèmes et les réseaux le plus rapidement possible.

Concernant l'organisation, on observe que tous les secteurs ont pris conscience de la nécessité d'élever leur niveau de sécurité. C'est ce qu'on appelle une mutation technologique.

Mais lorsque survient un dysfonctionnement, qui est le responsable ? Le pirate bien sûr, mais aussi le dirigeant de l'entreprise, le responsable des systèmes d'information ou tout simplement l'utilisateur qui a été négligent ou a fait une erreur de manipulation ? On a besoin de savoir dans chaque situation qui est responsable et qui supervise et coordonne le service qualité de la chaîne de réponse aux incidents.

M. Mickaël Vallet. **–** Le premier point est en effet d'élever le niveau de sécurité par la diffusion la plus large de ce qu'on peut appeler une hygiène numérique. Ensuite, cette prise de conscience générale doit être organisée et coordonnée.

La commission a émis un avis favorable à l'adoption des crédits du programme 129 de la mission « Direction de l'action du Gouvernement ».

II. AUDITION DE M. STÉPHANE BOUILLON, SECRÉTAIRE GÉNÉRAL DE LA DÉFENSE ET DE LA SÉCURITÉ NATIONALE, DU GÉNÉRAL DE BRIGADE AÉRIENNE EMMANUEL NAËGELEN, DIRECTEUR ADJOINT DE L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION ET DE M. MARC-ANTOINE BRILLANT, CHEF DU SERVICE DE VIGILANCE ET DE PROTECTION CONTRE LES INGÉRENCES NUMÉRIQUES ÉTRANGÈRES (18 OCTOBRE 2023)

Au cours de sa réunion du mercredi 18 octobre 2023, la commission des affaires étrangères, de la défense et des forces armées, sous la présidence de M. Cédric Perrin, président, a procédé à 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 la 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), sur la coordination des politiques de défense et sécurité nationale, de cybersécurité et de lutte contre les menaces hybrides.*

M. Cédric Perrin, président. – Monsieur le Secrétaire général, Mon Général, Monsieur le chef de service, mes chers collègues, dans le cadre de l'examen du projet de loi de finances pour 2024, nous accueillons M. Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale (SGDSN), pour l'entendre sur les crédits du programme 129 relatifs à la coordination des politiques de défense et sécurité nationale, de cybersécurité et de lutte contre les menaces hybrides. Je vous remercie de votre présence à un horaire qui est habituellement dédié aux réunions du Conseil de défense et de sécurité nationale dont vous assurez l'organisation ; vous étiez cependant aujourd'hui disponible car l'urgence de la menace terroriste a conduit à avancer le dernier conseil de défense.

Vous êtes accompagné 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). Je souligne que depuis votre audition de l'année dernière l'état-major qui vous entoure a été entièrement renouvelé puisque M. Vincent Strubel, représenté aujourd'hui par le Général Naëgelen, a remplacé M. Guillaume Poupard à la tête de l'ANSSI en début d'année. Plus récemment, M. Brillant a pris la relève de M. Gabriel Ferriol.

S'agissant de Viginum, qui a été créé il y a seulement deux ans, l'occasion est propice à dresser un premier bilan de son action dans un domaine, celui de la lutte contre les ingérences étrangères en matière de manipulation de l'information, que le Président de la République a érigé en priorité stratégique dans la revue nationale stratégique et dont on voit aujourd'hui encore un peu plus combien elle a d'importance. Je ne cache pas

que ce que vous pourrez nous dire de Viginum, dont le rôle reste relativement discret, peut-être à juste titre, m'intéressera particulièrement.

Vous nous direz également, Monsieur le Secrétaire général, comment vous entendez développer les missions de l'ANSSI pour faire face aux menaces de cybersécurité qui concernent notre sécurité nationale mais aussi chaque citoyen de notre pays. Des attaques très graves ont perturbé les services publics, collectivités territoriales et établissements de santé. Je pense que chacun d'entre nous a entendu parler dans sa circonscription d'attaques ou de dégâts intervenus dans ce domaine.

Je ne serai pas plus long car mes collègues auront certainement beaucoup de questions à vous poser et, en particulier, Olivier Cadic et Mickaël Vallet qui ont été reconduits dans leurs fonctions de rapporteur sur le programme 129.

Je rappelle que l'audition porte sur la cybersécurité et les menaces hybrides. Compte tenu du contexte sécuritaire, il y aura peut-être des questions en rapport avec la menace terroriste mais je vous laisserai juge d'y répondre au regard de vos attributions.

Avant de vous céder la parole, je rappelle à tous que cette audition fait l'objet d'une captation vidéo qui est retransmise en direct sur le site internet du Sénat.

M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale. – Je suis heureux de retrouver votre commission pour la quatrième fois, et de rencontrer à nouveau les sénateurs avec qui j'ai eu l'occasion de travailler tout au long de ma carrière. C'est à chaque fois un vrai plaisir de pouvoir vous informer de ce que nous faisons ou préparons, des moyens dont nous disposons et de la manière dont nous essayons de faire face aux crises auxquelles est confronté notre pays. Comme vous l'avez rappelé, Monsieur le Président, ces crises sont nombreuses et se sont encore accrues ces derniers jours. Ainsi lors du dernier Conseil de défense qui s'est tenu exceptionnellement vendredi dernier, nous avons proposé à la Première ministre de passer en urgence attentat. Cette décision a été prolongée par un ensemble de mesures prises dans notre pays : je pourrai vous donner plus de détails à leur sujet.

Tout d'abord, je vais vous présenter succinctement notre projet de budget pour l'année 2024. Le Secrétariat général de la défense et de la sécurité nationale (SGDSN) représente plus du tiers du total des crédits de la mission Direction de l'action du Gouvernement. Le budget opérationnel de programme (BOP) SGDSN représente ainsi 40 % des allocations du programme, 36 % des crédits du titre 2 consacrés aux dépenses de personnel et 43 % des crédits hors titre 2. Pour l'année 2024, nous vous proposons un budget de consolidation qui progressera, par rapport à 2023, de 4,8 % en autorisations d'engagement (AE) et de 11,8 % en crédits de paiement (CP).

Ce budget opérationnel sera ainsi porté à 363,5 millions d'euros en AE et 362,9 millions d'euros en CP.

Comme d'habitude, environ un tiers de ce budget est constitué par des dépenses de rémunération tandis que les deux tiers restants correspondent à des dépenses de fonctionnement et d'investissement. On constate des augmentations de dépenses imputables à la hausse des factures d'électricité, un accroissement des dépenses de travaux interministériels et une augmentation des moyens de Viginum, pour accompagner sa montée en puissance, ainsi que de l'ANSSI, en particulier pour lui permettre de faire face à la préparation des jeux Olympiques de 2024. Notre schéma d'emploi triennal pour la période 2024-2027 est respecté, avec 56 ETP (Équivalents Temps Plein) supplémentaires prévus en 2024, dont 40 au profit de l'ANSSI et 10 pour l'opérateur des systèmes d'information interministériels classifiés (OSIIC). Ce dernier est confronté à une hausse de charges liée à l'ensemble du matériel destiné aux communications intergouvernementales ou entre administrations : ces dernières doivent être protégées contre des ingérences étrangères qui se multiplient. Par ailleurs, des emplois supplémentaires sont prévus pour le GIC (Groupement interministériel de contrôle) et Viginum récupérera 17 ETP par voie de transfert, dont 10 ETP provenant du ministère de l'Intérieur et 7 ETP provenant du ministère des Armées. Ces emplois, qui étaient auparavant pourvus par voie de mise à disposition, seront totalement intégrés dans le Service de vigilance, ce qui lui permettra de renouveler ses effectifs et de compléter ses moyens. Au total, ce sont 1 283 ETP, dont 350 militaires, qui vous sont proposés par ce budget au sein du SGDSN. Je signale que le poids des restes à payer demeure élevé malgré nos efforts de réduction. Cela s'explique par les opérations immobilières importantes que nous menons. Ainsi, l'immeuble de l'ANSSI à Rennes, qui sera inauguré dans les prochains jours, accueillera à terme 200 personnes. Nous avons également renouvelé le bail pour les locaux de Viginum – c'est-à-dire le bâtiment dit du Ponant, en face de l'Hôpital Georges Pompidou. De plus, des travaux de réaménagement à l'intérieur des locaux du SGDSN sont en cours pour réhabiliter d'anciens bâtiments et les rendre utilisables.

J'en viens aux sujets d'actualité que vous avez évoqués, Monsieur le Président. La guerre en Ukraine a occupé une grande partie de notre année 2023 et cette tâche se poursuit. Nous avons également dû faire face aux effets des sanctions économiques et aux préoccupations en matière de sécurité économique. De plus, le non-respect du droit international et l'attitude de la Russie ont désinhibé les États autoritaristes, ce qui a suscité des menaces liées à la prolifération nucléaire, bactériologique et chimique. J'ajoute que les conflits frontaliers se sont réveillés dans de nombreuses régions, soulevant des questions relatives au droit de la guerre. En Afrique, la Russie a étendu son influence par la manipulation de l'information, ce qui a mobilisé Viginum tout au long de l'année. Le terrorisme islamique n'a malheureusement pas disparu malgré nos victoires contre l'État islamique au

Levant et il réapparaît dans notre pays ainsi que chez nos voisins. L'attaque terroriste du Hamas contre Israël, avec d'épouvantables massacres de civils, entraine d'ores et déjà des difficultés politiques, géopolitiques et humanitaires extrêmement graves. Nous sommes également attentifs à la l'influence croissante de puissances régionales comme l'Iran ou la Turquie et, bien entendu, la Chine nous préoccupe beaucoup, y compris en matière de cybersécurité et de désinformation.

Notre objectif est d'éviter de tomber dans le piège résumé par la formule « The West against the Rest » que certains veulent nous tendre, et qui vise à opposer l'alliance de l'OTAN, des États-Unis et des pays occidentaux au reste du monde. Cette tentative politique, qui est à l'évidence menée, est très dangereuse et nous souhaitons la contrecarrer fortement pour continuer à remplir notre rôle diplomatique de puissance d'équilibre dans l'ensemble du monde.

Par ailleurs, les enjeux climatiques commencent à avoir de fortes conséquences en termes de conflits et de migrations. Les sujets de démographie, que j'avais déjà évoqués devant vous ces dernières années, sont en train de monter en puissance : on le constate de facto avec les conséquences des guerres, mais aussi dans différents pays. Enfin, dans les 15 prochains mois, se profilent de nombreux calendriers électoraux qui seront une opportunité de rebattre les cartes, mais également l'occasion pour des adversaires d'essayer de nuire à la sincérité des scrutins. Je mentionne ici d'abord nos élections européennes. Tout le monde pense également aux élections américaines, britanniques – qui se dérouleront d'ici un an - aux élections sénégalaises, indiennes et russes, même si les résultats de ces dernières sont un peu moins incertains. Les enjeux de ces scrutins seront très importants et je rappelle que des élections viennent de se dérouler en Pologne.

Face à ces défis, nous devons renforcer nos protections. Je ne reviendrai pas ici sur la loi de programmation militaire que vous avez évoquée et que vous avez votée, pour laquelle nous avions préparé une revue nationale stratégique présentée en novembre 2022.

Je voudrais insister sur quelques menaces qui nous ont beaucoup occupés cette année. Avant de passer la parole à mes adjoints sur les thématiques de déstabilisation de l'information et de cybersécurité, j'aborderai les sujets de sécurité économique. Nous avons constaté des tentatives de prise de contrôle d'entreprises - après parfois leur déstabilisation - d'une ampleur extrêmement importante de la part de différents pays et dans différents endroits. Au moment où nous essayons de reconstruire notre industrie pour disposer d'une économie résiliente – la relocalisation industrielle et la reconstruction d'un tissu économique fort étant une nécessité dictée par l'évolution géopolitique - nous constatons l'existence de nombreuses activités visant à contrecarrer cette orientation, et, à tout le moins, à prendre le contrôle de nos entreprises. Je mentionne à cet

égard l'espionnage industriel, le débauchage d'ingénieurs et de commerciaux mais aussi l'utilisation de ce que nous appelons l'extraterritorialité du droit ou « lawfare » (qui renvoie au warfare), la judiciarisation des relations commerciales et l'édiction de normes internationales au bénéfice d'un État. Toutes ces actions nuisent à la sécurité économique en mettant en danger notre patrimoine scientifique, technique et économique.

Nous tenons très régulièrement des réunions non seulement avec le ministère de l'Économie et des Finances, mais également avec tous les autres ministères, y compris ceux concernés par la base industrielle et technologique de défense (BITD), pour protéger nos entreprises, réagir en soutenant leur capital, en intervenant à un moment ou à un autre ou en bloquant les investissements étrangers potentiellement hostiles, de façon à préserver une bonne partie de nos entreprises stratégiques. Nous organisons également des réunions mensuelles sur ce sujet avec le Service de l'information stratégique et de la sécurité économiques (Sisse) au sein du comité de liaison en matière de sécurité économique (Colise), et nous en organisons encore une cet après-midi pour examiner le cas d'un certain nombre d'entreprises en difficulté.

Nous menons également des campagnes de sensibilisation auprès de ces entreprises pour les inciter à la prudence, que ce soit en matière de cybersécurité - car certaines d'entre elles font preuve d'une naïveté désarmante - ou en matière de manipulation de l'information. Nous constatons en effet que, surtout dans le cadre du conflit actuel, il peut y avoir des activités de déstabilisation et de lutte contre la réputation qui peuvent être extrêmement puissantes.

S'agissant des ingérences numériques étrangères, je laisserai Marc-Antoine Brillant détailler l'ensemble du sujet : je souligne ici qu'il a eu énormément de travail et que celui-ci a été très bien conduit, mais de ce fait, il y a encore énormément d'opérations dont le traitement nécessite de nous réorganiser. Cette année, nous allons donc essayer d'avancer sur des sujets de stratégie, en liaison avec le ministère de l'Europe et des Affaires Étrangères ainsi que les autres ministères, pour élaborer une stratégie de lutte contre les manipulations de l'information. Il s'agit de développer non seulement notre capacité à réagir – je rappelle que, de même que l'ANSSI, Viginum a été conçue comme un bouclier et pas une épée - mais aussi de renforcer notre efficacité en coordonnant nos actions avec l'ensemble des acteurs susceptibles d'intervenir. Nous allons engager un travail sur ce sujet. 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.

Vous avez évoqué, M. le Président, les évolutions de l'état-major et il est vrai que deux postes majeurs ont changé de titulaire cette année. Je précise qu'au sein du SGDSN, nous avons également une nouvelle directrice de la protection et de la sécurité de l'État (PSE) : il s'agit de Mme Muriel Nguyen qui était auparavant directrice du cabinet ministériel de M. Olivier Klein après avoir été préfète de la Meuse puis de la Somme. Demain, j'aurai également à choisir une nouvelle personne à la tête de la direction des affaires internationales, stratégiques et technologiques (AIST) : le poste est actuellement vacant car M. Charles Touboul a rejoint le cabinet du Garde des Sceaux. Ainsi avec le chef du service des affaires générales, c'est en fait tout l'état-major, sauf votre serviteur et son adjoint, qui auront changé en 2023.

M. le général de brigade aérienne Emmanuel Naëgelen, directeur adjoint de l'Agence nationale de sécurité des systèmes d'information (ANSSI).- Dans le prolongement des propos du secrétaire général, je vous propose un premier tour d'horizon de la menace cyber, telle que nous l'observons, avant de vous présenter rapidement les deux principaux défis qui nous attendent dans les prochains mois.

En ce qui concerne la menace cyber, comme Guillaume Poupard l'avait mentionné l'année dernière, le niveau de menace est très élevé et il l'est resté en 2022. Plus encore, au premier semestre 2023, nous avons constaté une augmentation de 23 % du nombre d'événements traités par l'ANSSI par rapport au dernier semestre de 2022.

Nous continuons à faire face à trois types de menaces : une menace étatique ou stratégique, une menace de nature criminelle et une menace de type « hacktiviste ». La menace étatique ou stratégique, qui est le « fonds de commerce » de l'Agence depuis sa création en 2009, a pour principale finalité l'espionnage et elle se traduit également par du sabotage. Cette activité est celle qui occupe le plus les équipes de l'Agence. Je précise que sur les 19 opérations de cyberdéfense et incidents majeurs traités par l'ANSSI en 2022, neuf impliquaient des modes opératoires, c'est-à-dire des groupes, en source ouverte affiliés à la Chine.

Pour sa part, la menace d'origine criminelle est indiscriminée et massive. Elle s'est industrialisée en pratiquant ce qu'on appelle « la pêche au chalut », avec un fort impact sociétal comme en témoignent les attaques portées contre les hôpitaux. Cette criminalité a pour objectif l'extorsion de fonds en prenant en otage des données ou des systèmes d'information. Nous avons constaté une augmentation significative de cette menace au premier semestre 2023, avec une hausse de 50 % par rapport au dernier semestre de 2022. Les principales victimes sont les entreprises, notamment les TPE, les PME et les entreprises de taille intermédiaire, ainsi que les collectivités territoriales.

Enfin, la menace de nature revendicative est conduite par les « hacktivistes » qui cherchent à obtenir une couverture médiatique en

menant des attaques pour rendre certains sites web indisponibles. On a constaté une véritable résurgence de cette menace avec le conflit en Ukraine et plus récemment au Proche-Orient. Cependant, depuis les attaques du Hamas du 7 octobre dernier, nous n'avons pas observé d'augmentation des assauts informatiques touchant la France alors que de nombreuses opérations d'activisme contre Israël ont été menées par des groupes pro-palestiniens, pro-russes ou pro-iraniens.

Je signale enfin que nous observons une véritable porosité entre les groupes cybercriminels et les groupes étatiques, avec des convergences en termes de techniques. Ces attaques sont souvent rendues possibles en exploitant trois catégories de vulnérabilités : la principale est, tout d'abord, logicielle, les victimes n'appliquant pas les correctifs préconisés par les éditeurs, permettant ainsi d'exploiter des failles notoires. La deuxième se rattache à des usages informatiques mal maîtrisés et, enfin, les sous-traitants disposant de faibles protections sont une troisième source de vulnérabilité informatique.

J'en viens aux défis qui nous attendent. Les chiffres que je viens de vous donner parlent d'eux-mêmes et force est de constater que nous ne sommes pas en mesure aujourd'hui de couvrir totalement cette menace grandissante. Or l'objectif qui nous a été fixé par le président de la République dans la revue nationale stratégique est de donner à la France une cyber résilience de premier ordre. Pour atteindre cet objectif, nous devons relever un défi qui est vraiment structurel pour l'agence : celui du passage à l'échelle. En effet, la multiplication de nos moyens par deux, cinq ou dix ne nous permettrait pas, en l'état actuel, de répondre à la menace. Il faut désormais passer d'une logique très ciblée sur les opérateurs critiques, comme cela a été le cas jusqu'à présent, à une stratégie beaucoup plus large qui nous permettra de couvrir les établissements publics, les collectivités et les entreprises, avec des niveaux de protection adaptés à ces diverses entités. Ce passage à l'échelle nous impose aussi de travailler de plus en plus en réseaux et d'animer ces derniers, notamment au sein des régions. Grâce à France Relance, nous avons ainsi pu contribuer à la création de centres cyber dans 12 régions ainsi que de centres cyber dédiés à certains secteurs d'activité comme la santé, l'aviation ou le secteur maritime. Je mentionne ici également l'acteur extrêmement important qui préexiste à cette évolution et accomplit un travail formidable, à savoir « Cybermalveillance.gouv.fr ». Prenant appui sur l'existence d'acteurs émergents ou préexistants, l'enjeu consiste désormais pour nous à les faire travailler en réseau pour élargir au maximum la couverture du territoire en intégrant également les prestataires privés qui montent en compétence et se développent de plus en plus.

Ce passage à l'échelle pour déployer une cybersécurité de masse est conforme à l'esprit de la directive NIS 2 (Network and Information Security) que nous avons soutenue lors de la présidence française de l'Union européenne et qui doit être transposée d'ici 2024. Pour vous donner un

chiffre qui illustre bien ce passage à l'échelle, la directive NIS 2 va nous faire passer de 500 opérateurs aujourd'hui régulés par l'agence à environ 15 000, ce qui implique vraiment un changement de nos méthodes de travail. L'Agence va donc vivre une véritable révolution industrielle et, pour reprendre les mots de notre directeur général, il va nous falloir continuer à faire du sur-mesure, en particulier pour les opérateurs critiques ou les administrations les plus les plus régaliennes de l'État, mais aussi, désormais, du prêt à porter de qualité qui protège convenablement des attaques cyber.

Le deuxième grand défi auquel va être confrontée notre résilience nationale est évidemment celui des jeux Olympiques, avec une illustration très concrète du changement d'échelle que nous allons devoir mettre en œuvre. Comme pour les précédentes olympiades, nous sommes absolument convaincus que les prochains jeux Olympiques qui se tiendront à Paris vont concentrer sur notre pays un niveau inédit d'attaques cyber de tous ordres. Quantitativement, pour l'ANSSI, ces jeux Olympiques représentent 350 entités, dont 80 sont critiques, en ce sens que si ces 80 dernières subissaient une attaque informatique d'ampleur, une épreuve sportive ou une grande partie des Jeux pourraient être annulée. Beaucoup de ces acteurs n'ont jamais été confrontés au niveau de menace que j'ai mentionné et nous devons donc mener avec eux un travail massif de sécurisation pour les aider à monter en compétence à l'égard de ces risques. Pour vous citer quelques chiffres, la stratégie que nous menons actuellement, comporte une soixantaine d'audits et autant de plans d'action qui devront être terminés très rapidement à la fin du premier trimestre de 2024. Il s'agit également d'un exercice massifié de gestion de crise : puisqu'il nous est impossible de fournir un entrainement personnalisé à chacun de ces trois cent cinquante acteurs, nous leur distribuons des kits d'entraînement et nous les accompagnons à la gestion de crise. Cette utilisation massive de nos services automatisés d'audit vise à aider ces acteurs à mettre en place des plans d'action solides. Au-delà de ces entités, nous avons, par exemple, recensé 210 établissements de santé qui seront à proximité des sites de compétition, et dont nous devons nous assurer qu'ils sont bien sécurisés dans le cadre des plans d'action menés par le ministère de la santé. Nous nous intéressons également aux Services Départementaux d'Incendie et de Secours (SDIS) et vous avez certainement en mémoire l'exemple du SDIS64 (Pyrénées-Atlantiques), qui a subi une attaque extrêmement importante. En parallèle, nous mettons en place toute une mécanique opérationnelle pour nous assurer que nous serons capables de communiquer très rapidement avec l'ensemble des centres d'opérations qui vont gérer les Jeux Olympiques.

Enfin, la principale difficulté est que ces Jeux se dérouleront en deux fois 15 jours, avec les Jeux Olympiques suivis des jeux Paralympiques ; or en deux semaines, on ne peut pas reconstruire un système d'information qui aurait été détruit par un rançongiciel. Cela impose, d'une part, de miser sur une détection la plus efficace possible des attaques pour pouvoir les enrayer le plus tôt possible et limiter leurs éventuels impacts. D'autre part, nous

devrons mettre en place une sorte de médecine de guerre cyber, avec des plans de remédiation très rapides ainsi que des prestataires prêts à intervenir et réparer le plus vite possible les systèmes d'information qui auront été attaqués. Aujourd'hui, pour paraphraser une réplique d'une série TV des années quatre-vingts (consacrée à une Agence tous risques), notre « plan se déroule sans accroc » : mais nous nous situons aujourd'hui dans la partie la plus facile de notre plan d'action et ce qui nous attend à partir du printemps sera très certainement très différent.

M. Marc-Antoine Brillant, chef du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum). - Un rapide propos liminaire me permettra, tout d'abord, de replacer la mission du service Viginum dans un cadre plus global : celui d'un changement radical du contexte géopolitique, fondé sur un usage aujourd'hui décomplexé du rapport de force, avec pour instruments des actions de nature hybride dont la menace informationnelle est l'essence même.

Depuis une vingtaine d'années, nous assistons à un véritable durcissement des relations internationales qui les rapproche davantage d'une compétition stratégique désinhibée - c'est-à-dire d'une dialectique de puissance et entre puissances - avec pour caractéristique majeure le rapport de force. Nous sommes donc probablement entrés dans une ère géopolitique au sens réaliste du terme, c'est-à-dire une période d'affrontement indirect, de recherche de puissance pour imposer sa volonté par l'influence, l'intimidation, voire l'agression, parfois dans une logique opportuniste, et souvent de contournement.

Dans cette mêlée mondiale où tous les coups sont permis, les démocraties sont à la fois contestées et fragilisées face à des compétiteurs - qu'ils soient étatiques ou non - usant de tous leurs attributs, la technologie et les réseaux sociaux pouvant parfois jouer un rôle égalisateur. Les démocraties sont contestées dans leurs valeurs et leurs héritages - on le voit notamment sur le continent africain ; elles sont également fragilisées dans leur modèle, ce qui est en particulier le cas pour les démocraties libérales qui ont pour fondement l'ouverture et le respect des libertés.

C'est dans cette rivalité que naissent et s'épanouissent les menaces hybrides. Constituant un véritable défi pour la stabilité et la sécurité, la menace hybride se nourrit des périodes d'incertitude, entre guerre et paix, comme celle que nous vivons aujourd'hui. Cette menace estompe la frontière entre l'influence et l'ingérence en agissant par divers moyens et modes opératoires, souvent en-deçà du seuil de conflictualité, et en ciblant ou exploitant notre fonctionnement démocratique, notre cohésion sociale, notre économie ainsi que notre système normatif. De plus, ce que nous interprétons aujourd'hui comme nos forces sont en réalité des vulnérabilités du point de vue de l'adversaire et de nos compétiteurs.

Ce constat n'est pas nouveau puisqu'il a été parfaitement établi, comme vous l'avez opportunément mentionné, M. le Président, dans la revue

nationale stratégique publiée l'année dernière par le secrétariat général de la défense et de la sécurité nationale. Après avoir rappelé le contexte dans lequel se situe la menace informationnelle, permettez-moi à présent de vous en présenter un état actualisé.

De quoi parle-t-on ? Il s'agit d'un instrument qui est parfaitement intégré dans les stratégies hybrides de nos compétiteurs, sous forme de manipulations d'informations ou de manœuvres informationnelles mises en œuvre de manière délibérée et coordonnée. Elles visent - à l'aide de procédés techniques déloyaux comme des automates, qu'on appelle des bots, des trolls, ou des systèmes comme le copié-collé - à amplifier des contenus manifestement inexacts ou trompeurs dans notre débat public numérique.

Lorsqu'elles impliquent des acteurs étrangers, étatiques ou non, et qu'elles ciblent les intérêts fondamentaux de la nation, tels qu'ils sont définis par les articles 410 -1 du code pénal ou L. 811-3 du code de la sécurité intérieure, ces manœuvres sont des ingérences numériques étrangères. Cette menace informationnelle fait peser une menace réelle et sérieuse sur notre fonctionnement démocratique ainsi que notre cohésion, car elle vise avant tout à produire des effets dans la vie réelle. Même s'ils utilisent ces procédés à travers des plates-formes en ligne, et donc dans des débats virtuels, nos compétiteurs poursuivent des objectifs concrets : détourner le citoyen du vote ou orienter le suffrage, attiser la contestation - parfois avec de la violence physique dans la rue - ou encore perturber l'économie réelle, comme l'a évoqué le secrétaire général, par la promotion de campagnes de boycott qui peuvent viser nos grandes entreprises à l'étranger.

Les acteurs de la menace informationnelle appuient et s'appuient sur des fragilités existantes, comme la défiance croissante à l'égard des institutions, la fragmentation sociale, qui peut être liée aux difficultés économiques, et l'érosion progressive de l'esprit critique pour construire leur manœuvre d'influence informationnelle. Ils exploitent certains faits marquants d'actualité ou de société pour attiser des sentiments puissants, comme la frustration, la victimisation ou l'exclusion et chercher in fine à polariser durablement les différentes composantes ou catégories de citoyens d'une même société.

Tendanciellement, ces manœuvres sont de plus en plus diffuses dans notre débat public numérique. Concrètement, elles ne sont plus seulement circonscrites aux élections et touchent aujourd'hui tous les sujets de société. Elles sont de plus en plus élaborées dans leurs modes opératoires - à ce titre, l'intelligence artificielle générative est un sujet de préoccupation - et plus difficile à détecter du fait de l'usage d'intermédiaires ou de relais. La frontière entre une opinion et une information manipulée par un acteur étranger deviendra probablement de plus en plus mince et difficile à détecter. Enfin, à la faveur des conflits et des guerres, la menace informationnelle gagne en intensité, non seulement par une diffusion de plus en plus massive et rapide de contenus visant à saturer notre débat, mais

aussi par la combinaison de campagnes correspondant à des natures et à des logiques différentes, avec des campagnes planifiées ou opportunistes.

En pratique, les modes opératoires auxquels on doit faire face aujourd'hui sont multiples. Ils peuvent concerner aussi bien la contrefaçon de contenus – ici encore l'intelligence artificielle permet d'y arriver avec beaucoup plus de facilité – en matière de désinformation électorale, de discrédit des institutions, voire d'usurpation d'identité, mais aussi d'amplification de narratifs, afin de ceinturer un débat. Certains d'entre eux combinent l'attaque informatique et la manipulation de l'information : je pense, en particulier, au fameux « hack and leak », c'est-à-dire le piratage des données suivi de leur diffusion / divulgation / révélation, parfois après en avoir manipulé le contenu.

Deux modes opératoires sont particulièrement suivis par la Viginum car ils semblent un peu plus difficiles à détecter. Le premier emprunte le canal de la sous-traitance, c'est-à-dire le recours à des structures privées ou à des réseaux informels, comme des communautés, pour conduire des manœuvres. Le défi posé par ce mode opératoire est bien entendu celui de la détection, mais aussi de l'imputation à un acteur. Le second mode opératoire qui soulève aujourd'hui des difficultés particulières est le « micro-ciblage », c'est-à-dire le ciblage d'une audience restreinte mais disposant d'un fort pouvoir de mobilisation, y compris dans la vie réelle.

Je souligne que la manipulation de l'information n'est pas l'apanage des seuls États : nous observons aussi un véritable phénomène de marchandisation de la désinformation, avec des acteurs privés issus du marketing digital ou de la communication, qui proposent désormais des prestations de services combinant cyber espionnage et influence.

Je souhaite à présent vous présenter un rapide panorama des grands acteurs et de leurs modes opératoires ainsi que de leurs stratégies qui visent les intérêts de notre pays, en évoquant tout d'abord la menace russe ou pro-russe. La France est l'une des cibles privilégiées des manœuvres menées par le dispositif informationnel russe, que ce soit sur le territoire national ou à l'étranger, en particulier sur le continent africain. Pour diffuser du contenu qui lui est favorable et discréditer ses adversaires, la Russie et ses « proxies », qui agissent par procuration, se basent aussi bien sur des acteurs étatiques - à l'instar de son réseau diplomatique ou de ses services de renseignement - que sur des relais et des prestataires. La Russie s'appuie ainsi sur plusieurs acteurs privés spécialisés dans le domaine de l'influence, comme par exemple l'entreprise « Structura » que nous avons dévoilée en juin dernier dans le cadre de la campagne « RRN » - du nom du site pro-russe RRN.world (Reliable Recent News) - menée avec le ministère de l'Europe et des Affaires étrangères. Bien entendu, je mentionne également dans cette même catégorie, la galaxie d'opérateurs de feu Evgueni Prigojine. La Russie a un large panel de modes d'action et utilise des avatars sur les réseaux sociaux pour diffuser du contenu de propagande. Les principaux narratifs

utilisés aujourd'hui sont, d'une part, l'instrumentalisation du contexte politique et social sur notre territoire national et, d'autre part, la critique de notre passé colonial sur le continent africain.

Quelques mots, enfin, sur la menace pro-chinoise, avant d'aborder la mission de Viginum et ses principaux enjeux. Les stratégies d'influence informationnelle chinoise dans le débat public sont contrôlées et menées par l'État-parti et ses stratégies s'inscrivent dans le temps long. Elles ont pour principal objectif de défendre les intérêts de la France auprès d'une audience francophone et de diffuser une image positive de la puissance chinoise. La Chine affiche également une volonté de discréditer les États-Unis et l'OTAN, ainsi que de remettre en cause le modèle occidental.

Face à ce panorama, la France n'est pas restée inactive puisqu'elle a renforcé progressivement son dispositif national défensif, à travers, tout d'abord, en début d'année 2018, une première gouvernance interministérielle présidée par le secrétaire général de la défense et de la sécurité nationale - regroupant les principaux ministères régaliens - qui vise à fluidifier le partage d'informations, mieux comprendre les phénomènes auxquels nous faisons face et proposer des options de réponse. De plus, à la fin de l'année, l'arsenal législatif a été perfectionné avec les deux lois du 22 décembre 2018 qui renforcent à la fois les pouvoirs de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) et du juge des référés. À l'issue des attentats de Conflans-Sainte-Honorine en 2020 et de Nice, il a été également été décidé, en 2021, de doter le SGDSN d'un opérateur dédié et de modifier, dans le code de défense, les missions du SGDSN, avec à la fois une mission d'identification des opérations d'ingérence numérique étrangère et une mission d'animation de coordination des travaux de protection. Pour ce faire, le SGDSN dispose d'un opérateur dédié : Viginum.

Pour conclure, voici quelques mots sur les principaux enjeux pour Viginum dans les prochains mois. En plus de ce qu'a évoqué, s'agissant de l'ANSSI, le général Naëgelen sur les élections européennes et les JO, Viginum, sur la période 2023, a pour ambition d'asseoir et de consolider son rôle de référent national en matière de protection contre les campagnes numériques de manipulation de l'information, en élevant notre niveau d'expertise technique et en nous ouvrant de nouvelles perspectives en matière de partenariat stratégique. C'est pourquoi nous avons initié cette année un premier forum d'ouverture vers le monde académique et nous souhaitons aujourd'hui poursuivre cette démarche, non pas seulement pour mieux travailler des centres de recherche mais aussi parce que nous sommes résolument convaincus que cela contribuera à une meilleure information du grand public sur cette menace informationnelle.

Nous souhaitons aussi également mieux coordonner l'ensemble des acteurs issus des différentes sphères d'action, que ce soient les sphères d'action publique, privée et de la société civile pour, in fine, mieux renforcer la résilience de la société face à ces phénomènes. Enfin, nous nous attellerons

à accroître la coopération avec nos partenaires étrangers et internationaux, afin d'avoir un meilleur partage d'informations et, peut-être, demain, de mieux anticiper la menace.

M. Stéphane Bouillon.- Juste un mot, si vous le permettez, pour dire que tout ceci nous amène à travailler sur les sujets de résilience, c'est-à-dire de résistance de notre pays, en anticipant sur ce type de crise cyber ou géopolitique. Nous sommes en train de mettre en place une stratégie nationale qui concerne non seulement l'État, mais aussi les collectivités locales. Nous sommes en train, avec les mairies, les départements et les régions, de regarder comment nous pouvons travailler ensemble, comme nous avons réussi à le faire lors de la crise du Covid en 2020 – certes, au début de cet épisode, on a un peu « patouillé » mais, par la suite, on a réussi à faire face à cette crise Covid en travaillant avec les collectivités locales. C'est ce que nous essayons à nouveau de faire aujourd'hui, en anticipant et en associant ensuite les citoyens afin que ceux-ci puissent jouer pleinement leur rôle auprès des maires, des départements et de l'État, pour être non seulement des consommateurs de sécurité mais aussi des acteurs de sécurité.

M. Cédric Perrin, président. – Je remercie les intervenants et voudrais rappeler à l'ensemble de nos collègues ainsi qu'à tous ceux qui nous écoutent le rôle majeur que jouent vos agences dans la guerre de haute intensité que le chef d'état-major avait théorisée mais qui, malheureusement, n'est plus une théorie : elle consiste d'abord à gagner la guerre avant la guerre, ce qui implique d'être prêt, ou en tout cas disponible et actif sur les questions de lutte cyber, informationnelle ou numérique. Vous êtes des acteurs majeurs dans ce domaine et c'est pourquoi il est très important de pouvoir vous écouter aujourd'hui. Le calendrier parlementaire nous impose aujourd'hui d'examiner les questions budgétaires mais au vu des enjeux majeurs que notre pays doit relever, nous aurons certainement l'occasion de vous entendre à nouveau sur ces questions de cybersécurité.

Je laisse à présent la parole d'abord à nos deux rapporteurs et ensuite à l'ensemble des commissaires.

M. Olivier Cadic. - Je remercie à mon tour nos trois intervenants pour la clarté de leur propos. Notre audition fait l'objet d'une diffusion publique, et pourtant vous n'avez pas hésité à appeler un chat, un chat et à caractériser les États qui ne nous veulent pas que du bien : il est intéressant que vous puissiez ainsi véhiculer une bonne information. De plus, cela fait maintenant plusieurs années que nous nous voyons et, au fil du temps, ces auditions nous donnent l'impression d'être écoutés et entendus : je voudrais donc vous remercier doublement.

J'en viens à ma première question : entre les quelque 831 intrusions répertoriées en 2022 par l'ANSSI dans sa publication annuelle du panorama de la cybermenace dont vous avez fait état, et les 170 000 demandes d'assistance reçues par le GIP ACYMA Cybermalveillance, une clarification

mérite d'être apportée afin de bien comprendre la stratégie du SGDSN pour atteindre l'objectif de la revue nationale stratégique d'une résilience cyber de premier rang, aussi bien pour les opérateurs d'importance vitale (OIV) que les PME, les collectivités et les particuliers. Nous avons bien compris que, pour le haut du panier, l'application de la directive européenne dite NIS 2 devrait conduire l'ANSSI à décupler son champ de compétence : on part donc d'environ 700 OIV actuellement suivis par l'agence et, d'après les estimations, vous indiquez que 15 000 entreprises seraient concernées lorsque la directive sera transposée d'ici fin 2024. Nous souhaiterions savoir comment vous allez relever ce défi et réaliser ce passage à l'échelle industrielle de la cybersécurité. Avez-vous dressé un calendrier de transposition de cette directive, une liste des obligations nouvelles qui pèseront sur les entreprises, et une estimation du coût qu'elles devront supporter ? Quels services l'ANSSI leur apportera-t-elle ?

La semaine dernière, j'étais à Washington où l'ancien président de Paypal nous a indiqué que cette entreprise subissait trois à quatre millions d'attaques par jour, ce qui illustre le niveau de risque auquel les entreprises sont confrontées. À l'autre extrémité du spectre, il faut prendre en compte le grand public, les collectivités, les PME, les TPE et les associations ; or les moyens du GIP Cybermalveillance se limitent à une quinzaine de personnes avec un budget de seulement deux millions d'euros : tout cela nous semble dérisoire pour couvrir l'ensemble des besoins. Quels objectifs fixez-vous à ce groupement, notamment s'il est appelé à gérer le futur guichet unique 17 Cyber que le Sénat appelle de ses vœux depuis maintenant cinq ans, que nous attendons toujours, et dont je rappelle que le président de la République l'a aussi demandé il y a deux ans. Entre ces deux spectres, vous avez créé des centres régionaux de réponse cyber, encouragés et financés dans le cadre du plan de relance. Leur montée en puissance est lente et leurs services sont très inégaux, d'après les remontées de terrain. De plus, leur financement par l'État n'est pas pérenne et on comprend mieux pourquoi la région Auvergne-Rhône-Alpes n'est pas entrée dans le dispositif. Les autres régions, notamment la Nouvelle-Aquitaine, redoutent de devoir reprendre à leur charge des missions de sécurité qu'elles estiment régaliennes. Quelle réponse apportez-vous sur le financement et la coordination de ces centres régionaux ? Disposez-vous d'un bilan de leurs actions ?

Enfin, je voudrais partager avec vous une réflexion : j'étais il y a trois semaines à Taïwan et j'ai rencontré l'homologue du SGDSN. Je souligne que Taïwan est certainement aujourd'hui la première destination des attaques en provenance de la Chine, où l'influence et l'ingérence se combinent. Ce pays est un peu le laboratoire mondial des attaques cyber car une fois testées sur Taïwan, des attaques analogues se retrouvent après partout dans le monde. De ce fait, Taïwan organise des exercices internationaux cyber : je ne vais pas vous demander si vous y participez mais je voudrais savoir si vous prenez part à des exercices internationaux dans ce domaine.

M. Mickaël Vallet. – Vous avez évoqué au début de votre intervention la question des jeux Olympiques. Je voudrais que vous puissiez nous préciser plus en détail votre positionnement et votre rôle à l'égard des aspects de cybersécurité que nous allons devoir assurer dans le cadre de cet événement. L'actualité et les tensions actuelles rehaussent les risques et la sécurité des jeux, dans toutes ses dimensions y compris les punaises de lit, est un sujet pour l'opinion publique. Quel est votre rôle vis-à-vis du comité d'organisation et de la collectivité parisienne ? Quels sont les principaux prestataires vers lesquels vous êtes tourné et quels types de préparation doivent-ils assurer face à quels risques - si tant est que vous puissiez identifier lors d'une audition publique les menaces qui vous semblent les plus importantes, pour éviter de donner des idées à des personnes malveillantes ?

Je souhaite néanmoins vous interroger sur votre stratégie d'organisation pour les JO et je fais ici le lien avec ma question suivante : en effet, il nous a été expliqué au cours de précédentes auditions qu'au final, les scrutins les plus importants que nous avons connus récemment, comme l'élection présidentielle, n'ont pas donné lieu à des attaques ou à une volonté de manipulation aussi manifestes que dans d'autres démocraties. S'agissant du référendum en Nouvelle Calédonie, on nous a également indiqué que, finalement, les ingérences, qu'on aurait pu attendre de la part des acteurs que vous avez cités, en l'occurrence les Russes, n'ont pas eu lieu. Je pense par conséquent que les jeux Olympiques seront un moment important pour évaluer notre dispositif et j'aurais voulu pouvoir vous entendre sur l'aspect vraiment pratique de cet enjeu.

Je souhaite également prolonger la question de mon collègue Olivier Cadic sur la façon de s'organiser entre les différentes strates, à savoir l'État, les régions et le GIP Cyber malveillance : il s'agit de veiller à ce que les uns ne supposent pas à tort que les autres sont chargés d'une tâche et qu'au final plus personne ne s'y attèle ; il ne faut pas non plus oublier les cas dans lesquels, avec une petite dose de mauvaise foi, on espère que l'autre va financer une activité dont on n'est pas soi-même chargé… Finalement, votre enjeu principal - et je souhaite savoir comment vous y faites face - n'est-il pas de développer l'hygiène et la culture du numérique ? En effet, une chose est de consacrer des moyens et d'installer des pare-feux de façon ponctuelle, mais tant que nous n'aurons pas une conscience globale, depuis les acteurs étatiques jusqu'au citoyen lambda, on va en quelque sorte vider l'océan avec une petite cuillère. Comment, sur ce point, envisagez-vous une montée en puissance et je fais ainsi le lien avec les aspects budgétaires de votre action ?

Ma dernière question porte sur un point de vigilance signalé dans notre rapport de l'an dernier - dont nous ne doutons pas qu'il a retenu votre attention. Nous avions pointé la question des structures hospitalières outre-mer. Dans l'hexagone, en cas d'attaque cyber, il est parfois possible de basculer les cas les plus urgents d'un hôpital à l'autre – et je note au passage

que même en l'absence de cyber attaque, la pénurie actuelle de médecins en province impose, certains week-ends, des transferts de patients d'un hôpital à l'autre. S'agissant des outre-mer, avez-vous pris en compte nos remarques : estimez-vous qu'elles étaient trop alarmistes ou pas et quelles suites y avez-vous apporté ?

M. Olivier Cadic.- J'ajoute que, depuis la création de Viginum en 2021, il nous semble que ce service s'est montré un peu discret sur sa montée en puissance et sur la communication de ses résultats. Mis à part une communication notable du ministère des Affaires étrangères sur une affaire que vous avez évoquée, et qui concernait des activités russes en Afrique, quels éléments pouvez-vous nous fournir pour justifier l'activité et le développement du service?

M. Stéphane Bouillon.- Je commencerai par votre dernière question : Viginum a effectivement été discrète, tout particulièrement pendant la campagne présidentielle. C'était très volontaire, puisque nous étions avant tout au service du juge de l'élection. Par conséquent, nous avons rendu compte de tout ce que nous avons vu et détecté au Conseil constitutionnel, à la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle et à l'Arcom. Ensuite, nous ne bougions plus une oreille, si je puis dire, en attendant que le juge de l'élection décide ou pas d'en parler ou d'intervenir. Nous n'avons révélé au grand public l'opération « Beth » qu'après les élections, avec l'accord du Conseil constitutionnel, pour permettre aux journaux de savoir ce qui s'était passé. Tout au long des investigations et des relevés concernant cette opération suspecte ou d'autres, nous avons chaque fois, et presque chaque soir, fait passer par motard au Palais Royal l'ensemble des éléments dont nous disposions.

Nous souhaitons maintenant que Viginum développe son travail académique avec les think tanks et les universités pour pouvoir exploiter l'ensemble des informations dont nous disposons et travailler sur l'aspect éducatif à l'égard du grand public. S'agissant de vos propos sur les aspects cyber et sur la manipulation de l'information, il est absolument indispensable que nos concitoyens comprennent ce qu'ils voient sur internet ou ailleurs. Pour nous, la question de fond n'est pas de dire ce qui est vrai ou faux : je ne suis pas légitime pour le faire, et vraisemblablement, si je me prononçais, les gens comprendraient ou voudraient croire le contraire. Il s'agit simplement d'expliquer à nos concitoyens que quand ils pensent parler avec leurs voisins de Valenciennes, de Carpentras ou de La Rochelle, ils sont parfois en train de discuter avec un agent des services de renseignements installé à Ankara, à Pékin, ou en Russie. De plus, lorsqu'il peut sembler que des dizaines ou des centaines de milliers de personnes sont d'accord avec telle ou telle opinion, il faut expliquer que ces centaines de milliers d'interventions sont parfois nées d'un clic expédié à un moment précis et qui a déclenché quelques centaines de milliers d'ordinateurs

contrôlés à travers la planète. Ceci dit, si les gens veulent croire les informations qu'ils ont vues, c'est leur choix, et ce n'est pas notre rôle de dire si c'est vrai ou faux. Nous essayons simplement de démonter le mécanisme d'authenticité de l'information et c'est là-dessus que nous essayons également de travailler avec l'Éducation nationale. Nous allons également essayer de mettre en place avec le Centre national d'enseignement à distance une diffusion de tutoriels en s'inspirant de ce qui a été accompli en matière d'environnement en poussant fortement les feux sur ce sujet.

S'agissant des deux directives NIS 2 et « résilience des entités critiques » qui vont vous être présentées dans le courant de l'année 2024, nous avons d'ores et déjà engagé un travail interministériel sur les modalités de leur mise en œuvre et je précise que tant les entreprises que les collectivités locales seront concernées. Nous sommes en train d'examiner avec les grandes associations de collectivités locales le niveau de protection adapté pour protéger les uns et les autres car on ne va évidemment pas demander à une commune de 350 ou de 1 000 habitants de se protéger de la même manière que Lyon, Marseille ou une grande région. Pour en avoir discuté avec Sébastien Martin, président d'Intercommunalités de France, on sait aussi que lorsqu'une intercommunalité est attaquée, ce qui devient de plus en plus fréquent, l'intrusion passe généralement par les points les plus faibles et en particulier les petites collectivités. Nous allons donc avancer sur ce sujet, y compris en examinant comment utiliser les mécanismes de soutien aux collectivités locales dans ce domaine.

S'agissant des aides, je mentionne également les allocations du plan France Relance ainsi que plusieurs dispositifs sur lesquels nous allons vous apporter des précisions. Cependant, je souligne l'analogie entre la cybersécurité et la protection du domicile : c'est à chacun d'entre nous de prévoir et d'engager l'installation de serrures à mettre sur les portes, de barreaux aux fenêtres ou de coffres forts. Il en va de même pour les attaques cyber qui font malheureusement partie des menaces dont il faut désormais se prémunir. Siphonner les données d'une collectivité locale, c'est non seulement la mettre en danger en essayant d'obtenir une rançon mais cela permet aussi de vendre ces données sur le dark web à des malfaiteurs, d'attaquer les possesseurs de ces données ou de les réutiliser pour casser des codes et pénétrer d'autres systèmes informatiques. Chacun doit donc pouvoir jouer son rôle : nous le faisons et avons prévu les moyens d'amplifier notre action mais je pense que les collectivités locales, les entreprises et les particuliers qui font en sorte que leurs maisons ne soient pas cambriolées doivent également se prémunir contre le cambriolage de leurs données et processus informatiques.

M. Emmanuel Naëgelen. – Tout d'abord, je rappelle que NIS 2 est un texte crucial que nous avons impulsé lors de la présidence française de l'Union européenne. Nous y avons beaucoup travaillé et sommes très satisfaits de son contenu. L'objectif qui nous est fixé est de l'avoir transposé

impérativement d'ici le 17 octobre 2024 : le calendrier est donc assez tendu et nous vous soumettrons un texte au printemps 2024. D'ici là, nous allons engager plusieurs chantiers. Je fais d'abord observer que NIS 2 constitue une révolution à bien des égards et cela va nous obliger à dialoguer avec des PME, des ETI ainsi que des collectivités d'une taille que nous n'avions pas l'habitude de traiter. Or on ne communique pas avec un patron de PME ou avec un élu d'une petite commune comme on parle à un opérateur d'importance vitale ou à une grande administration. Ces acteurs ne disposent pas des mêmes moyens et nous devons donc trouver des solutions adaptées. Dans le courant du mois de novembre-décembre, nous allons engager une série de consultations pour partager plusieurs choses. La première est de définir la manière dont on va interagir avec tous ces nouveaux acteurs. Jusqu'à présent, nous avions une relation assez intime et des échanges réguliers avec les opérateurs critiques. Demain, avec 15 000 entités régulées, on ne pourra pas avoir ce même niveau de connaissance et de relation ; pour autant, il va bien falloir que ces entités se connaissent, sachent qu'elles sont désormais régulées et qu'elles ont des tâches à accomplir. Il faut donc adapter notre façon d'interagir avec ces nouveaux acteurs et nous allons lancer une consultation spécifique sur ce sujet. Une deuxième consultation va porter sur le périmètre : il s'agit de déterminer jusqu'où aller en termes de taille d'entreprise et de collectivités. Faut-il toutes les intégrer ou fixer un certain seuil ? C'est un sujet très important dont on va débattre et discuter avec les grandes associations et fédérations. Enfin, nous allons mener une consultation sur les règles applicables car, ici encore, on ne peut pas avoir le même niveau d'exigence pour un opérateur d'importance vitale et une PME. Il faut trouver des exigences efficaces mais atteignables compte tenu des moyens dont chacun dispose. Ces trois consultations visent à enclencher un débat constructif et à nous faire progresser sur ce sujet nouveau pour nous et sur lequel nous ne prétendons pas détenir a priori la vérité.

M. Stéphane Bouillon.- Juste un mot pour rappeler que la transposition des directives soulève régulièrement des difficultés analogues : les directives européennes sont conçues pour être prises en compte par des Länder, des grandes régions et quelques milliers de communes ou de départements, au grand maximum. Or en France, nous avons 36 000 communes et il faut donc que nous adaptions ces règles à notre manière de fonctionner, sans handicaper nos collectivités en leur imposant un fardeau excessif. Je ferai cependant observer que même si elles sont attaquables, d'une certaine manière, la petite taille des communes les protège : c'est un peu comme dans la jungle où on dit que quand on est poursuivi par un lion, le problème n'est pas tant de courir plus vite que le lion que de devancer son voisin. Sous cet angle, attaquer des petites collectivités représente un travail important mais ne rapporte pas grand-chose et il est peut-être plus rentable pour nos compétiteurs malveillants de s'attaquer à de plus grosses collectivités. Il faut donc mettre en place une protection minimale dotée

d'une certaine efficacité mais qui ne soit évidemment pas trop coûteuse pour les uns et les autres et n'entrave pas le mode de fonctionnement de nos collectivités. C'est tout le travail que nous engageons avec les associations d'élus et bien entendu avec vous.

M. Emmanuel Naëgelen. – Pour compléter et illustrer concrètement ce propos, l'ANSSI développe actuellement un service en ligne dénommé "Mon Service Sécurisé". Celui-ci proposera demain à une mairie qui n'a aucune expertise en cybersécurité un parcours, qu'on va accompagner pendant une ou deux heures, permettant par exemple de s'assurer que le service en ligne d'aide sociale que la commune souhaite mettre à la disposition de ses administrés ne va pas faire fuiter des informations personnelles. C'est là un outil et une approche un peu nouvelle pour nous destinée à aider les administrations, établissements publics et collectivités de petite taille à se poser rapidement les bonnes questions et à trouver un certain nombre de réponses élémentaires qui rejoignent la notion d'hygiène de cybersécurité que vous avez évoquée.

Concernant le dispositif Cyber malveillance et les CSIRT (Computer Security Incident Response Team) régionaux ou sectoriels, je souligne que notre objectif est que chaque victime d'attaque cyber ait au moins un interlocuteur ou un intervenant à sa disposition. Nous sommes aujourd'hui très loin d'atteindre cet objectif de constitution d'un « jardin à la française » car nous n'avons n'a pas suffisamment d'acteurs locaux permettant effectivement d'apporter des réponses aux petites entités ou aux particuliers. À ce stade, l'enjeu est de faire pousser des arbres dans notre jardin ; quand on en aura suffisamment, nous pourrons veiller à ce qu'ils soient bien taillés, disposés en lignes droites et que chacun ait un périmètre bien défini. Pour l'instant, notre priorité est d'arriver à faire émerger le plus grand nombre d'acteurs possible. Vous avez indiqué que les CSIRT ne sont pas encore complètement opérationnels et nous en avons bien conscience mais nous nous situons dans une phase d'accompagnement de ces scénarios régionaux de protection cyber pour qu'ils deviennent très rapidement les plus opérationnels et efficaces possible dans leur ressort. À l'issue de cette montée en puissance, on pourra dans dix ans se poser des questions de périmètre extrêmement précises mais nous n'en sommes pas encore là.

M. Stéphane Bouillon.- J'ajoute que le ministère de l'Intérieur, avec la gendarmerie et la police, a mis en place un service à compétence nationale ainsi que toute une organisation destinée à aider les collectivités locales et les particuliers, en particulier dans la lutte contre la cyberdélinquance.

Je précise également que l'ANSSI a été désignée comme pilote de la lutte contre les cyberattaques lors des jeux Olympiques. Un dispositif est donc mis en place et il fonctionnera 24 heures sur 24 pendant les JO. D'ores et déjà, il est actif, avec un système d'astreinte pour répondre aux questions des uns et des autres. L'ANSSI s'occupe des 80 opérateurs très sensibles que nous avons évoqués : il s'agit principalement des stades – dont nous avons

observé que certains nécessitent des correctifs – et des systèmes de transports. Ensuite, nous avons un deuxième cercle dans lequel l'ANSSI surveille des entreprises privées au service de ces opérateurs, pour les aider, les tester, les accompagner et évaluer la situation. Dans un troisième cercle, encore un peu plus éloigné, nous effectuerons des sondages pour vérifier que tout le monde a bien pris en compte les mesures requises, sachant qu'au cours du processus de contractualisation avec ces entreprises, il leur a été demandé d'être attentives à la cybersécurité. La question se posera, y compris en matière de marchés publics, de savoir si, dans le cahier des charges, on ne doit pas demander aux entrepreneurs de prévoir des mesures de sécurité permettant de ne pas paralyser les services publics voisins. On sait par exemple que, dans les hôpitaux, c'est parfois à travers des entreprises extérieures et des fournisseurs que la porte dérobée a été ouverte et, donc, que tel ou tel hôpital a été attaqué malgré toutes les précautions qu'il avait pu prendre. Il faudra réfléchir à ce sujet et c'est sans doute un des aspects sur lesquels le Parlement devra se prononcer.

M. Marc-Antoine Brillant. – En réponse à votre question sur les données justifiant l'activité de Viginum, je peux tout d'abord rappeler quelques chiffres issus du premier rapport public du service de vigilance, publié en fin d'année dernière. En 2022, nous avons travaillé sur environ 140 phénomènes que nous qualifions d' « inauthentiques », c'est-à-dire des comportements atypiques ou aberrants, des contenus trompeurs, ou des comptes et des profils présentant des caractéristiques d'inauthenticité. Sur ce total de 140, le service a caractérisé une douzaine d'ingérences numériques étrangères qui, par définition, visent à amplifier de manière artificielle et automatisée des contenus inexacts ou trompeurs avec la finalité d'atteindre les intérêts fondamentaux de la nation.

Le secrétaire général a également mentionné le phénomène Beth intervenu pendant l'élection présidentielle : nous avons pu le rendre public à travers un documentaire télévisé de Complément d'enquête. Plus récemment, pendant l'été 2023, vous avez pu prendre connaissance de la fameuse campagne que nous avons baptisée RNN qui visait, dans le cadre de la guerre Russie-Ukraine, à usurper l'identité de vrais médias et de sites officiels, comme celui du Quai d'Orsay, pour diffuser du contenu totalement faux. Par ce procédé, les internautes qui surfent sur les réseaux sociaux, tombent à un moment sur un site qui ressemble à s'y méprendre à un site institutionnel ou à un site de média officiel, sauf, évidemment, que le contenu n'est pas du tout le même. Telles sont les données assez précises que nous avons pu publier et qui justifient l'activité du service.

S'agissant de la discrétion de Viginum, et pour compléter les propos du secrétaire général, le service de vigilance vient de fêter son deuxième anniversaire : il est donc très récent. L'impératif qui nous était assigné et la directive qui m'a été donnée était, dans un premier temps, de créer une capacité opérationnelle crédible. Nous avions ainsi un devoir d'humilité

pendant les deux premières années du fonctionnement du service car notre effort consistait à crédibiliser et à mettre cette nouvelle capacité opérationnelle à l'épreuve des élections ainsi que d'autres événements, ce qui justifie également la relative discrétion que nous avons observée jusqu'à présent.

M. Cédric Perrin, président. – Avant de laisser la parole aux autres commissaires, je voudrais revenir rapidement sur la question posée par Mickaël Vallet sur les JO et les moyens supplémentaires mis à votre disposition. Pouvez-vous nous indiquer si vous l'avez volontairement éludée : peut-être ne souhaitez-vous y répondre qu'à huis clos ?

M. Emmanuel Naëgelen. – Voici plusieurs précisions. Tout d'abord, **d**ans le cadre de la loi 19 mai 2023 relative aux Jeux Olympiques et Paralympiques de 2024, 10 millions d'euros nous ont été alloués pour sécuriser les entités critiques précédemment évoquées. Concrètement, en ayant recours à des prestataires privés, nous avons réalisé un certain nombre d'audits qui nous ont permis de commencer à élaborer des plans d'action. Notre objectif est que d'ici la fin du premier trimestre 2024, ces plans d'action soient réalisés car nous serons alors très proches de l'échéance et il sera difficile de continuer à sécuriser.

M. Joël Guerriau. – On assiste à un tsunami de l'information et il est toujours difficile d'y détecter les fake news : bien souvent, les petits messages très courts qui sont aisément retenus par notre cerveau sont les plus efficaces. Nous avons bien mesuré, à travers les constats que vous nous avez présentés, la difficulté de lutter contre ce phénomène. Vous avez évoqué la loi du 22 décembre 2018 relative à la lutte contre la manipulation de l'information : sur la base de vos constatations, avez-vous des suggestions de perfectionnements législatifs pour renforcer encore davantage notre sécurité cyber ?

Ce qui m'inquiète également beaucoup, ce sont les informations très agressives qui conduisent à passer de la violence virtuelle à la violence réelle tout en générant un phénomène de désensibilisation de nos populations à des actes de violence, en raison d'une accoutumance à des réseaux qui en portent énormément. Là encore, quelles sont à votre avis les possibilités d'évolution des normes pour renforcer nos chances de lutter contre ces phénomènes ?

M. François Bonneau. – Avant tout merci pour vos exposés. Je voudrais plus spécifiquement aborder le sujet de l'intelligence artificielle et de l'IA générative - qu'on peut aussi nommer automatisation numérique puisqu'il ne s'agit pas stricto sensu d'intelligence. Toujours est-il qu'aujourd'hui, l'IA n'en est qu'à ses débuts et il s'agit d'un défi redoutable lancé à nos États. Comment envisagez-vous de répondre à ce qui va devenir un véritable bouleversement ?

M. Ludovic Haye.- Je vous remercie à mon tour pour avoir dressé, dans un temps record, un panorama numérique très précis sur un sujet qui ne l'est pas forcément. J'aurais de nombreuses questions à vous poser mais je vais m'en tenir ici à l'aspect quantitatif de la donnée numérique.

Aujourd'hui, comme vous le savez, la quantité est bien souvent l'ennemi de la qualité et le numérique n'échappe pas à cette règle. Les chiffres parlent d'eux-mêmes et, sans vous abreuver de chiffres, je rappelle qu'il y a trois ans, nous avons atteint soixante zettabytes de données, c'est-à-dire 10 puissance 21 : c'est un saut considérable à l'ère où, dans certaines entreprises, on compte encore en gigas, c'est-à-dire en milliards ou 10 puissance 9. On a beau changer d'unités, l'explosion des données reste spectaculaire puisqu'on devrait atteindre 180 zettabytes l'année prochaine.

J'ajoute que la France n'échappe pas à une sorte de syndrome de Diogène numérique : concrètement, on ne vous reprochera jamais de produire ou de stocker de la donnée. En revanche, dans une entreprise ou une entité publique, le jour où vous supprimez une donnée cruciale, on ne manquera pas de vous retrouver et cette tendance participe à l'explosion des données.

Je rappelle également que le cycle de la donnée ne s'arrête pas à sa production ni à son stockage mais se poursuit normalement jusqu'à sa suppression, sauf si on peut justifier sa réutilisation, ce qui relève du RGPD (Règlement Général sur la Protection des Données). Je souhaite vous interroger sur le thème suivant : à l'ère du big data et du data lake, l'IA et le quantique l'informatique vont bien entendu nous permettre de traiter des données toujours plus importantes ; cependant ne serait-il pas opportun de « se mettre au régime » dès maintenant, si tant est que, dans vos fonctions respectives, il est toujours plus simple d'être efficace et précis en gérant des données maîtrisables que des données qu'on ne maîtrise pas. Comment, dans les fonctions qui sont les vôtres, pensez-vous pouvoir juguler cette fuite en avant, pour autant que ce soit possible ? Je suis bien conscient que, comme vous l'avez suggéré, cette explosion des données est liée à celle de la démographie et au fait que de plus en plus de personnes acquièrent chaque année des appareils connectés qui produisent des données.

M. Stéphane Bouillon.- S'agissant des aspects législatifs et réglementaires, j'ai constaté en relisant récemment la loi du 29 juillet 1881 sur la presse qu'à peu près tout est déjà dedans. En particulier elle impose d'identifier qui écrit, qui publie et qui édite. De plus, ce qui est écrit et publié doit respecter les lois en vigueur, et en tout cas ne pas nuire à la paix publique. Depuis, on s'est toujours conformé à cette logique et la loi que vous avez votée en 2018 va dans le même sens.

Ceci dit, il faut sans doute améliorer un certain nombre de choses et, en particulier, la capacité dont nous pouvons disposer à aller chercher des

données et, le cas échéant, à pouvoir pénétrer dans ces données. Lorsque vous avez voté la LPM, nous vous avons proposé plusieurs dispositions permettant de placer des marqueurs dans certains serveurs, de pouvoir chercher certaines données afin de vérifier s'il n'y a pas des intrus et d'être en mesure de maîtriser des attaques ciblées. Grâce à vous, nous avons donc déjà pu renforcer un peu notre action et il faudra que nous puissions regarder si, compte tenu de l'évolution, notamment avec l'irruption de l'intelligence artificielle et du quantique, nous n'avons pas besoin de disposer d'autres outils très techniques : dans ce domaine, je suis un peu dépassé et je vais passer avec soulagement le relais à mes voisins pour préciser ce point.

Je souhaite simplement ajouter que l'intelligence artificielle et le quantique, constituent à la fois une menace, qui peut conduire à de sérieux dérèglements, mais aussi un atout car cela peut nous permettre de déceler plus facilement des fake news ou des attaques et faciliter nos interventions. Dans ce domaine, il faudra donc pouvoir établir des règles strictes, tout en utilisant ces outils afin de protéger la liberté d'opinion et la liberté d'expression.

M. Emmanuel Naëgelen. – L'intelligence artificielle soulève pour nous trois défis principaux. La première question est de savoir si l'intelligence artificielle pourrait demain permettre de mener plus facilement des attaques informatiques. Nous constatons aujourd'hui, que ce n'est pas encore le cas puisqu'on n'a pas encore observé d'attaque informatique générée par une intelligence artificielle mais je ne peux pas vous dire que ce ne sera pas le cas demain. Le deuxième défi porte sur les moyens de protéger ces intelligences artificielles et ces algorithmes : c'est une vraie question car il faut veiller à ce que ces IA continuent à fonctionner comme prévu et qu'elles ne produisent pas des résultats aberrants ou biaisés. C'est un sujet très difficile sur lequel nous n'avons pas encore les idées claires. Le troisième enjeu est d'utiliser l'intelligence artificielle pour mieux se protéger. C'est un outil précieux que nous utilisons déjà, car pour faire une bonne cybersécurité, il faut collecter des données techniques - qui ne sont pas identifiantes ni des données portant sur les contenus - mais des données techniques pour détecter des comportements anormaux qui seraient des signes précurseurs d'une attaque informatique. Nous avons ainsi besoin de collecter énormément de données et l'intelligence artificielle est un outil qui nous permettra de trouver une aiguille dans une botte de foin, pour identifier des débuts d'attaques cyber qui méritent d'être investiguées.

M. Marc-Antoine Brillant. – Juste quelques compléments portant sur la loi de 2018. Je mentionne d'abord que le projet de loi visant à sécuriser et réguler l'espace numérique (SEREN), aujourd'hui en discussion, renforce un certain nombre d'obligations. Il faut également prendre en compte la mise en œuvre future du Digital Services Act (DSA ou règlement européen sur les services numériques) qui introduit de nouvelles exigences notamment à l'égard des opérateurs de plateformes en ligne. L'enjeu pour nous est, dans

un premier temps, d'examiner comment ces différents dispositifs vont s'articuler pour ensuite déterminer si d'autres modifications législatives pourraient être nécessaires. Je me félicite de la ligne directrice du DSA (Digital Services Act) et du projet de loi SEREN, selon lesquels ce qui est illégal dans la vie réelle doit l'être également dans la vie numérique.

En ce qui concerne l'intelligence artificielle, je partage totalement les propos des deux autres intervenants : certes, on observe l'émergence de nouvelles menaces par le biais de l'intelligence artificielle et en particulier des modèles génératifs. Cela se manifeste d'abord par l'animation de faux comptes et d'avatars de manière beaucoup plus fluide, ensuite dans la génération de contenus de qualité pouvant passer en dessous des seuils de détection des plateformes de détection, et enfin dans le potentiel de diffusion massive de données pour saturer un débat public. Cependant, l'intelligence artificielle nous est utile, en tant que bouclier, pour renforcer nos capacités de détection. Nous pouvons ainsi imaginer des projets, en collaboration avec certaines structures, pour développer des outils de détection de deepfakes, c'est-à-dire des vidéos fabriquées par l'intelligence artificielle. Au total, l'IA peut être utilisée autant comme un glaive que comme le bouclier que nous sommes. Nous avons d'ores et déjà engagé des travaux d'amélioration de nos capacités de détection.

M. Olivier Cadic. – Pour aller dans votre sens, je signale que, la semaine dernière, le cadre dirigeant en charge de l'intelligence artificielle chez Facebook devenu Meta a indiqué qu'en 2017, pendant la campagne présidentielle, 20 à 25 % des discours de haine ont été supprimés grâce à l'IA. Aujourd'hui cette proportion atteint 95,6 %, ce qui confirme vos propos.

M. Patrice Joly.- Ma question porte sur « la menace à la menace ». Je m'explique : vous avez évoqué le dispositif défensif que vous mettez en place et je souhaite savoir si vous avez également une mission offensive. Il s'agit de s'interroger sur notre façon d'agir, conformément aux valeurs que nous portons, pour soutenir les mouvements démocratiques des pays qui nous attaquent ainsi que pour informer les populations concernées en relevant et en dénonçant la manipulation et la maltraitance dont elles sont victimes.

M. Roger Karoutchi.- Monsieur le Secrétaire général, un de vos propos introductifs m'a interpellé lorsque vous avez évoqué la nécessité de ne pas tomber dans le « piège » qu'essaye de nous tendre les ennemis du bloc OTAN- Occident. Or j'ai plutôt cru comprendre que la Chine, la Russie, l'Iran, la Turquie entraient dans un bloc anti occident, ce qui constitue un nouveau rapport de force mais pas particulièrement un piège. Qu'entendez-vous par ce dernier terme ?

M. Stéphane Bouillon.- Tout d'abord, en réponse au sénateur Patrice Joly, je précise que la difficulté du combat contre la désinformation réside dans le fait que celle-ci constitue une menace totalement asymétrique.

Par exemple, dans nos démocraties, si une attaque cyber frappe un transport en commun, le président de la RATP et le ministre sont immédiatement convoqués, interrogés, et on leur demande de rendre des comptes. En revanche, dans telle ou telle capitale que je ne citerai pas, on va considérer qu'une panne de métro, c'est normal et de toute façon, personne n'osera poser la question de savoir pourquoi elle s'est produite et quand elle sera réparée, parce qu'au final de tels incidents sont fréquents. Il en va de même en matière de manipulation de l'information c'est la même chose : il est absolument impossible de pouvoir communiquer dans ces différents États où il n'y a pas de liberté de presse. Nous essayons malgré tout de le faire puisque le dispositif France 24 ou RFI diffusent des informations par les ondes ou par internet et peuvent atteindre le grand public. Au-delà, je sors, si je puis dire, de mon domaine de compétence car le SGDSN a pour objectif de protéger : encore une fois nous sommes le bouclier mais pas l'épée. Nous sommes néanmoins en contact avec l'épée et peut-être pourrez-vous interroger la ministre Catherine Colonna que vous entendez cet après-midi sur notre potentiel offensif. En effet, la ministre a mis en place une stratégie d'influence, avec le ministère des Armées, qui vise à faire passer un certain nombre d'informations, non seulement sur la politique et les actions que nous menons, mais aussi pour essayer de majorer notre rôle d'épée. En tout état de cause, la menace demeure asymétrique entre la démocratie que nous sommes et certains pays qui ne le sont pas.

S'agissant du piège « the West against the Rest » sur lequel s'interroge le sénateur Karoutchi, je souligne que l'expression a été en quelque sorte inventée par un ou deux des pays que vous venez de citer. Cette formulation ne nous était pas venue à l'esprit et d'ailleurs quand nous travaillons avec nos partenaires – hier encore, j'étais à l'OTAN - nous estimons toujours avoir un rôle de soutien, de développement et de partage ou d'extension de nos valeurs. Cependant, certains autres pays essayent au contraire d'accréditer l'idée que ce schéma est complètement dépassé, que la démocratie n'est pas un bon système pour l'ensemble des nations de la planète et que les occidentaux sont des colonialistes avant tout soucieux de conserver leur pouvoir ou leur emprise, etc. Tel est le piège dans lequel nous devons éviter de tomber ; par conséquent, à travers les politiques et les actions que nous menons dans le cadre de l'OTAN, du G7 et sur le plan diplomatique, nous devons justement faire en sorte qu'un certain nombre de pays ne tombent pas dans ce traquenard et ne nous rangent pas dans une catégorie imaginaire inventée pour servir les intérêts de nos adversaires et certainement pas les nôtres.

M. Cédric Perrin, président. – Au terme des prises de parole de mes collègues, je m'étonne parfois aussi, comme notre collègue Mickaël Vallet, que, dans la perspective des jeux Olympiques, la question des punaises de lit - qu'il convient évidemment de ne pas négliger – prenne pour certains plus d'importance que notre capacité opérationnelle de lutte anti-drone, par exemple ; peut-être, aurons-nous l'occasion d'y revenir ultérieurement.

J'aurais également une petite question à formuler. Parmi mes principales inquiétudes, figure le projet de scission d'Atos qui soulève de très nombreuses interrogations, tant sur les conséquences pour notre souveraineté nationale d'une éventuelle vente à un investisseur étranger, que sur des enjeux cyber et stratégiques. Je rappelle qu'un certain nombre d'acteurs et de salariés d'Atos sont détenteurs d'habilitations au secret défense. Comme vous le savez, j'assure avec plusieurs de mes collègues, un suivi très attentif de cette opération et ce depuis bien avant le début du mois d'août dernier. Pouvez-vous, Monsieur le Secrétaire général, nous préciser votre rôle et les moyens d'action qui sont mis à votre disposition dans cette délicate affaire ? À titre personnel, il me semble qu'on a très peu entendu – publiquement en tous cas - les services concernés par cette opération qui a des retentissements sur la sécurité nationale, notre capacité de lutte cyber et les jeux Olympiques dans lesquels Atos s'est particulièrement impliquée - c'est le moins qu'on puisse dire. J'ajoute que l'interrogation de Mickaël Vallet sur les moyens mis à disposition de vos services pour les Jeux Olympiques appelle peut-être également des précisions sur les missions déléguées à Atos, avec des conséquences potentiellement critiques. Pouvez-vous nous dire un mot à ce sujet ? Bien entendu, d'autres questions peuvent être soulevées, comme celle des supercalculateurs mais l'essentiel ici pour nous porte sur la sécurité nationale dans laquelle Atos est partie prenante, avec les conséquences que cela peut avoir aujourd'hui.

M. Stéphane Bouillon.- Je vous avoue que j'aurai un peu de mal à répondre complètement à votre question, Monsieur le Président, mais je ne manquerai pas de la relayer auprès de l'ensemble des interlocuteurs avec qui je suis amené à avoir des réunions de travail sur ce sujet. Comme vous l'avez rappelé, Atos nous aide en matière de cybersécurité pour les JO, et l'ANSSI a eu un rôle non négligeable pour faire en sorte que le RGPD soit respecté par les prestataires des services informatiques pour les JO, ce qui a amené à choisir l'entreprise française plutôt que l'entité prévue par le Comité International Olympique (CIO); ATOS donc pas celui qui était prévu par le CIO.

M. Cédric Perrin, président. – Je rappelle qu'ATOS a également été un des acteurs majeurs pour les Jeux Olympiques de Tokyo.

M. Stéphane Bouillon.- Tout à fait. Par ailleurs, nous sommes évidemment très sensibles à la question des supercalculateurs qui sont indispensables pour notre dissuasion nucléaire, à quoi s'ajoutent bon nombre d'autres services informatiques.

Dans la situation actuelle, le rôle du SGDSN consiste donc à rappeler, un peu comme vous venez de le faire, nos intérêts fondamentaux et que la solution qui doit être trouvée pour l'avenir d'Atos doit nécessairement intégrer la capacité de celle-ci - ou de la nouvelle entreprise qui lui succédera - de préserver intégralement notre souveraineté, notre capacité d'innovation, d'intelligence ainsi que de production de systèmes informatiques et de

calculateurs performants pour notre dissuasion. Je suis désolé de ne pas pouvoir vous en dire plus sur ce thème, mais j'ai soigneusement pris le message.

M. Cédric Perrin, président. – Je pense que ce message circule depuis un certain temps et je rappelle, dans cette audition qui fait l'objet d'une diffusion publique, que nous réfléchissons très sérieusement – certes en fonction de la manière dont les choses se dérouleront et je note ici qu'elles viennent de bouger - à mettre en place une commission d'enquête sur ce sujet qui retient tout particulièrement notre attention.

Monsieur le Secrétaire général, mon général, Monsieur le chef de service, merci beaucoup pour vos interventions et surtout pour la sincérité d'un certain nombre de vos propos - je peux comprendre que ce soit compliqué sur des sujets comme celui d'ATOS. Je me félicite que vous ayez pu clairement décrire un certain nombre de menaces qui étaient jusqu'à présent connues mais peu caractérisées. Compte tenu des menaces et des enjeux mondiaux qui se manifestent quotidiennement, cette audition en appellera vraisemblablement d'autres. Vous avez beaucoup parlé de votre rôle de bouclier et un peu moins de celui de l'épée : ce sera peut-être l'occasion de vous entendre dans des conditions plus propices à nous donner davantage d'informations.

LISTE DES PERSONNES AUDITIONNÉES

Auditions de la commission

Mercredi 18 octobre 2023 :

– **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 la 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).

Déplacements et auditions des rapporteurs

Jeudi 14 septembre 2023 :

- **MM. Vincent Strubel**, Directeur général de l'ANSSI, **Mathieu Feuillet**, sous-directeur des opérations, **Gwenaël Jezequel**, conseiller du SGDSN et **Mme Jennyfer Chrétien**, directrice de cabinet.

Mardi 31 octobre 2023 :

- **M. Jérôme Notin**, GIP ACYMA Cybermalveillance.

Lundi 6 novembre 2023 :

Déplacement à Lyon avec le **Colonel Patrice Tromparent**, membre du cabinet du ministre des armées en charge du cyber et du numérique (cybercercle, visite de l'école de cybersécurité « CSB.School » et du Centre interarmées des actions sur l'environnement).

Mercredi 8 novembre 2023 :

- **MM. Patrick Guyonneau**, directeur de la sécurité du Groupe Orange, **Jean-Marie Mele**, directeur de la sécurité de l'information du Groupe et **Mme Carole Gay**, Responsable des relations institutionnelles à la Direction des Affaires Publiques ;

- **M. José-Francisco Araujo**, global chief technology officer d'Orange Cyber Défense ;

- **M. Pierre-Yves Jolivet**, vice-président « solutions de cyberdéfense » du Groupe Thales et **Mme Caroline Morenas**, chargée de mission à la direction des relations institutionnelles.

Mardi 14 novembre 2023 :

- **M. Pascal Chauve**, directeur du groupement interministériel de contrôle (GIC).

Mercredi 15 novembre 2023 :

- **M. Florent Kirchner**, coordinateur de la stratégie nationale cyber du Secrétariat général pour l'investissement (SGPI).