ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Mercredi
20 mai 2026
Séance de 11 heures

Compte rendu n° 69

SESSION ORDINAIRE DE 2025-2026

Compte rendu

Commission de la défense nationale et des forces armées

– Audition, ouverte à la presse, de M. Emmanuel Lebrun-Damiens, directeur de la communication et de la presse au Ministère de l'Europe et des Affaires étrangères, et de Mme Anne-Sophie Dhiver, cheffe de service adjointe du Service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM) du SGDSN (cycle « Guerre hybride et continuum de conflictualités ») 2

Présidence de M. Loïc Kervran, *Vice-président*

ASSEMBLÉE NATIONALE

La séance est ouverte à onze heures deux.

M. Loïc Kervran, président. Mes chers collègues, nous avons le plaisir d'accueillir M. Emmanuel Lebrun-Damiens, directeur de la communication et de la presse du ministère de l'Europe et des affaires étrangères, ainsi que madame Anne-Sophie Dhiver, chef de service adjointe du service de vigilance et de protection contre les ingérences numériques étrangères (Viginum) du secrétariat général de la défense et de la sécurité nationale (SGDSN).

La direction de la communication et de la presse joue un rôle stratégique dans la guerre informationnelle qui se déroule aujourd'hui en continu. Elle est en première ligne dans cette bataille des récits, des images, des perceptions qui touchent directement l'image et la perception de la France à l'étranger. Je pense par exemple aux mises en scène qui créent de fausses images, prêtent des propos fallacieux à des responsables politiques en utilisant l'intelligence artificielle (IA) ou encore aux nombreuses campagnes de désinformation qui ciblent la France de façon désinhibée, en particulier en période électorale.

Depuis plusieurs mois, le Quai d'Orsay a intensifié son réarmement en matière informationnelle. Je pense notamment au compte « *French Response* », qui permet de riposter aux attaques mensongères et rétablir les faits. Nous serons donc particulièrement intéressés à connaître les caractéristiques, les enjeux de cette lutte informationnelle et la manière dont vous y répondez.

Par ailleurs, le front numérique est celui sur lequel se joue principalement la lutte contre les ingérences étrangères et la désinformation, ce qui rend l'action de Viginum d'autant plus cruciale. Je rappelle ainsi que Viginum, rattaché au SGDSN, est chargé de la détection de la caractérisation des ingérences numériques étrangères. Il sera donc intéressant de vous entendre sur la mise en œuvre de la nouvelle stratégie nationale de lutte contre les manipulations d'information 2026-2030 élaborée par le SGDSN, et à laquelle notre commission et les groupes politiques ont contribué. Plus largement, nous souhaitons obtenir votre éclairage, sur le contexte actuel marqué par la multiplication des opérations de déstabilisation.

M. Emmanuel Lebrun-Damiens, directeur de la communication et de la presse au ministère de l'Europe et des affaires étrangères. Je vous remercie pour votre invitation et cette opportunité d'échanger avec la commission sur le rôle joué par le ministère de l'Europe et des affaires étrangères dans la guerre informationnelle.

Ce sujet est suivi par deux directions au ministère : la direction de la communication et de la presse (DCP), mais aussi la direction générale de la mondialisation, qui agit davantage sur la question de la résilience des sociétés, à travers un soutien aux médias, et notamment notre opérateur Canal France International, l'Agence française de développement médias. L'action de notre audiovisuel extérieur constitue une force, pour apporter une information indépendante, fiable et de qualité, pour promouvoir nos valeurs. Notre audiovisuel extérieur participe également à des actions de rétablissement des faits grâce à des programmes, face à des manipulations de l'information.

Ma présentation portera sur l'action de la direction de la communication et de la presse, à la fois notre action sur le volet défensif, mais aussi notre action proactive, sur le volet offensif. Permettez-moi tout d'abord de revenir brièvement sur l'évolution du champ

informationnel. En effet, celui-ci a fortement évolué ces deux dernières décennies. Il s'est fragmenté sous l'effet de deux phénomènes. D'une part, le poids de la presse intermédiaire a diminué au profit des réseaux sociaux, dont le développement a entraîné de phénomènes de bulles cognitives, de confinements algorithmiques. D'autre part, l'intelligence artificielle permet désormais la production d'hypertrucages, de *deepfakes*, à des coûts accessibles pour tous.

Nos adversaires et nos compétiteurs se sont engouffrés dans ces failles du champ informationnel, pour porter atteinte à nos intérêts. La brutalisation des relations internationales a fait du champ informationnel un champ de confrontation. La manipulation de l'information est devenue un risque systémique, dans un contexte de guerre hybride, au point que le Forum économique mondial considère par exemple la désinformation comme l'un des tout premiers risques mondiaux.

Le ministère de l'Europe et des affaires étrangères s'est attaché à répondre à cette situation à partir de 2021-2022, avec le développement d'une capacité de veille. Elle s'est traduite par la création, à la direction de la communication et de la presse, d'une sous-direction *ad hoc*, la sous-direction de la veille et de la stratégie ; mais aussi par le recrutement de profils adaptés et la dotation d'outils, logiciels, d'écoutes sociales. Nous avons également développé nos capacités de veille dans notre réseau diplomatique, par la formation des personnels des services de presse de nos ambassades, ainsi que l'identification de personnes chargées de cette veille au quotidien, tout autour du monde.

Notre réseau diplomatique, le troisième au monde, représente un capteur formidable, grâce auquel nous bénéficions d'une vision à 360 degrés du champ informationnel mondial, nous permettant une compréhension des menaces et une connaissance des acteurs. C'est donc sur cette capacité de veille du champ informationnel, développée de 2022 à 2024, que nous avons pu construire, sous l'impulsion du ministre Jean-Noël Barrot, une action plus résolue, faisant aujourd'hui du ministère de l'Europe et des affaires étrangères un acteur de protection des Françaises et des Français dans la guerre informationnelle.

La capacité à nous défendre face à des attaques constitue le volet défensif quand la capacité de porter nous-mêmes nos propres récits dans le champ des perceptions représente le volet proactif ou offensif. Concernant le volet défensif, nous travaillons dans un cadre interministériel, notamment avec le ministère des Armées et avec Viginum, en particulier sur le sujet des ingérences numériques étrangères, à travers des comportements inauthentiques, dont Viginum analyse le mode opératoire informationnel. Le cas échéant, le processus aboutit à l'attribution à une puissance étrangère.

Ces dernières années, nous avons également vu se développer des manipulations d'information de la part de comptes authentiques, qui ne recourent pas à des moyens d'amplification. Pour citer un exemple récent, dans les semaines qui ont précédé le sommet *Africa Forward* de Nairobi, nous avons repéré – en particulier dans des pays d'Afrique anglophone – des campagnes authentiques dans leur mode de propagation, qui insinuaient que la France envisageait de préparer des coups d'État néocoloniaux. Clairement, nos adversaires cherchaient à développer un sentiment anti-français à la veille de ce sommet, à manipuler l'information sur le terrain émotionnel, pour façonner le champ des perceptions.

Un deuxième exemple concerne la manière dont la Russie utilise le champ informationnel pour avancer ses pions en Ukraine, dans un contexte typique de guerre hybride, qu'il s'agisse de justifier son agression par un prétendu comportement offensif de l'Otan – *French Response* y a répondu très récemment – ou de faire croire que la situation de ses troupes sur le front est meilleure qu'elle ne l'est réellement.

La Russie utilise donc la manipulation de l'information pour obtenir dans le champ des perceptions du monde entier, et en particulier en Afrique, un résultat auquel elle ne parvient pas sur le champ de bataille. Notre travail consiste à repérer ces manipulations de l'information de la part de nos adversaires et compétiteurs, et d'y répondre.

Nous y répondons d'abord à travers notre réseau diplomatique, à partir des réseaux sociaux des ambassades. C'est en effet souvent le moyen le plus efficace de contrer une manipulation de l'information qui vise l'opinion publique d'un pays donné. À ce titre, vous avez certainement vu les actions mises en œuvre sur les réseaux sociaux de nos ambassades, ces derniers mois et années. Nous nous sommes également dotés d'un outil à Paris, *French Response*, que nous avons lancé sur X en septembre 2025, et que nous venons d'élargir à TikTok. Cet outil a connu un développement rapide : nous avons plus de 200 000 abonnés sur X aujourd'hui.

L'objectif de *French Response* consiste à redresser le champ des perceptions, quand il a été défiguré volontairement en notre défaveur. Nous le faisons en utilisant un ton particulier, parfois ironique, à la fois pour adopter les codes des réseaux sociaux, mais aussi dans un but de désescalade. Il ne s'agit naturellement pas de remplacer le langage diplomatique, mais de l'augmenter. C'est la raison pour laquelle nous avons créé un compte à part, à l'écart de nos réseaux sociaux institutionnels.

Nous investissons des espaces informationnels qui existent, où nous n'étions pas, et où nos adversaires et compétiteurs s'en prenaient à nos intérêts. Nos audiences sont très largement étrangères, ce qui est tout à fait en phase avec le rôle de ce compte, qui vise à répondre aux manipulations de l'information venant de l'étranger, en touchant les opinions publiques étrangères.

Après huit mois d'exercice, ce compte nous a permis d'atteindre deux réalisations. D'une part, nous disposons désormais d'un outil de réponse immédiate aux attaques, pour rétablir rapidement les positions françaises, en recadrant les informations déformées par nos compétiteurs. Cet outil est efficace, la réponse est visible. Dans certains cas, notre réponse entraîne le retrait des contenus que nous visons.

D'autre part, le deuxième effet est intervenu grâce à la très grande couverture médiatique : cette innovation *French Response* a incarné un changement de posture, montrant que la France ne se laissait pas faire. À ce titre, nous pouvons dire aujourd'hui que *French Response* est devenu un objet géopolitique, une voie nouvelle qui permet à la France de faire entendre ses positions dans le monde.

Mais nous ne voulons pas uniquement nous positionner dans la réaction, nous voulons également occuper nous-mêmes l'environnement informationnel. Face aux attaques, il faut être également présent de manière proactive. Nous avons d'ailleurs organisé le 7 mai un événement sur ce sujet, à la Gaîté Lyrique, qui avait été intitulé « Agir dans la bataille des récits ».

Nos adversaires se sont armés de récits pour servir leur projet géopolitique. Ces récits sont souvent simplistes et brutaux, mais ils participent à façonner les perceptions des opinions publiques internationales en leur faveur. En Russie, la fameuse doctrine Karaganov est bien connue. Mais nous voyons également émerger des récits venus d'ailleurs, par exemple de comptes Maga aux États-Unis, qui, à travers des récits réactionnaires, véhiculent des messages hostiles à notre modèle de société européen. Ces récits constituent des stratégies d'influence, qui cherchent à obtenir des gains géopolitiques. Ils alimentent une confrontation permanente dans le champ informationnel et rendent une communication institutionnelle de moins en moins audible.

Dans la guerre informationnelle, et comme l'a dit le ministre Jean-Noël Barrot dans son discours à la Gaîté Lyrique, les récits sont des armes. Pour nous, 2026 est donc l'année où le ministère s'engage dans la bataille des récits, et nous le faisons de plusieurs manières. D'abord, nous engageons ce travail avec nos ambassades, pour analyser les récits présents dans le champ informationnel local, et développer nos propres récits dans ce contexte. Pour y parvenir, nous avons créé une instance dans nos ambassades, sous l'autorité de l'ambassadeur, qui regroupe l'ensemble de ses services. C'est à travers cette instance que nous fixons nos priorités et nos stratégies narratives.

Ensuite, nous transformons la communication du ministère et de l'ensemble du réseau diplomatique, pour la rendre plus efficace et pour porter ces récits. Dans ce contexte, nous déployons une communication stratégique. Dans son organisation et ses modes d'action, elle doit nous permettre d'occuper plus efficacement le champ informationnel et d'assurer un impact plus important, que nous nous attachons davantage à mesurer. Tel est l'effet final recherché.

Le troisième élément concerne le recours à la société civile. Dans ce travail de définition et de déploiement de nos propres récits, la bataille est nécessairement une action collective. Ainsi, l'ensemble de la société doit être impliqué dans la réflexion sur les récits. À cet effet, nous constituons actuellement, sur une base expérimentale, le premier contingent de la réserve diplomatique, un contingent numérique dédié à la réserve informationnelle.

Nous avons déjà reçu plusieurs centaines de candidatures. Lors de l'événement à la Gaîté Lyrique, nos conseillers de presse avaient été mobilisés et ont pu faire passer des entretiens à ces candidats. Nous allons donc sélectionner plusieurs dizaines de réservistes, qui seront les premiers à participer à ce système, des compatriotes qui disposent de compétences qui viennent compléter et enrichir notre dispositif. Comme vous le voyez, l'objectif consiste bien à façonner nous-mêmes l'environnement informationnel, et non plus seulement de réagir aux lignes adverses.

M. Loïc Kervran, président. Je vous remercie. Je trouve assez frappant que vous utilisiez les termes de contingent, de bataille, d'armes, d'état final recherché (EFR) – soit un vocabulaire auquel nous sommes particulièrement habitués au sein de cette commission. Nous y voyons bien les manifestations de l'acculturation du ministère de l'Europe et des affaires étrangères à ce nouvel environnement.

Mme Anne-Sophie Dhiver, cheffe de service adjointe du service de vigilance et de protection contre les ingérences numériques étrangères du secrétariat général de la défense et de la sécurité nationale. Je vous remercie pour cette invitation, qui me donne

l'occasion d'aborder un volet spécifique de la guerre hybride, à savoir celui des manipulations de l'information d'origine étrangère, et plus précisément les enjeux récents liés à la protection de notre débat public numérique contre les ingérences numériques étrangères, qui constitue le cœur de l'action de Viginum.

Dans ce propos liminaire, je souhaiterais développer trois messages principaux. Le premier est le suivant : nous assistons aujourd'hui à une intensification sans précédent de la menace d'ingérences numériques étrangères. Celle-ci est à la fois croissante, persistante et multiforme. Les dix-huit derniers mois ont marqué, à cet égard, un point culminant particulièrement notable, comme nous avons pu le constater au quotidien dans nos activités.

Avant d'entrer dans l'analyse de cette menace, il convient d'en comprendre les facteurs d'accélération. Trois éléments principaux peuvent être identifiés. Le premier est d'ordre stratégique, avec le retour, depuis 2022, d'une compétition de puissances affirmée, qui conduit à un usage plus décomplexé des leviers hybrides par des acteurs étatiques et non étatiques.

Le second facteur est de nature systémique et tient à la transformation profonde du terrain numérique. Aujourd'hui, quatre Français sur dix s'informent via les réseaux sociaux. Cette mutation des usages offre de nouveaux vecteurs d'action à des acteurs malveillants, notamment grâce à des technologies comme l'intelligence artificielle, et elle s'accompagne d'une érosion progressive de la consommation des médias traditionnels, créant de nouvelles vulnérabilités.

Enfin, un troisième facteur tient à l'existence de crises persistantes, qu'elles soient géopolitiques, économiques ou sociétales. Ces tensions constituent autant d'opportunités exploitées par des acteurs étrangers pour tenter d'influencer et de polariser le débat public.

Dans ce contexte, les ingérences numériques étrangères s'imposent comme un instrument privilégié de stratégie hybride. S'agissant de la physionomie de cette menace, un premier élément saillant concerne la persistance d'acteurs étrangers malveillants au sein de notre espace informationnel, en vue de nous déstabiliser. Viginum suit aujourd'hui plusieurs dizaines de modes opératoires informationnels étrangers structurés, qui reposent sur des dispositifs techniques capables de diffuser de manière continue des opérations dans le débat public numérique. Ces actions combinent des contenus en ligne et, parfois, des actions dans le champ physique.

Elles poursuivent des objectifs variés, allant de l'affaiblissement de la cohésion nationale à la promotion de narratifs alternatifs, en passant par la déstabilisation de territoires, la promotion de vérités alternatives ou la mise en cause de nos intérêts économiques, industriels et sécuritaires.

Pour atteindre ces objectifs, ces acteurs étrangers malveillants, étatiques ou non-étatiques, recourent à une large palette de procédés visant à manipuler l'information numérique sur tel ou tel sujet. Il peut s'agir de la création de comptes inauthentiques, qu'il s'agisse de bots ou de trolls, de la production de contenus générés par intelligence artificielle, de la mise en place de sites web inauthentiques imitant des médias légitimes ou des institutions officielles, ou encore de campagnes d'amplification massive de contenus, parfois via des influenceurs rémunérés. Ces techniques visent à manipuler artificiellement la formation du débat public numérique. Je pense également à la publication massive de

contenus, l'*astroturfing*, en vue de remonter dans les algorithmes et d'augmenter la visibilité des contenus.

L'exemple du mode opératoire Storm 1516 illustre cette réalité. Attribué à un acteur russe, ce dispositif vise à affaiblir le soutien occidental à l'Ukraine, en ciblant notamment des audiences européennes, et notamment françaises. Il repose sur des procédés structurés, incluant la production de contenus audiovisuels, parfois avec recours à l'intelligence artificielle (IA), et l'usurpation de l'identité de médias. Ce mode opératoire a permis de mener plus de 200 actions contre les intérêts français au cours des deux dernières années, notamment lors des élections législatives de 2024 et des municipales de 2026.

Un second fait saillant concerne la professionnalisation croissante de cet écosystème. Elle se traduit par l'émergence d'acteurs intermédiaires spécialisés. Une première catégorie regroupe des « prestataires de l'inauthentique » qui peuvent fournir une série de services et de technologies aux opérateurs d'ingérence numérique étrangère pour anonymiser leurs opérations, puis amplifier de manière artificielle leurs actions sur les réseaux sociaux. Ces technologies peuvent servir notamment à générer par exemple des réseaux de bot, en vendant des lots de cartes SIM qui permettent de confirmer la création de comptes créés de manière massive puis à les animer de manière automatisée en fournissant des logiciels centralisés de pilotage automatisé de ces comptes inauthentiques.

Une seconde catégorie correspond à des prestataires proposant des services d'ingérence clés en main. Ainsi, certains acteurs privés sont en mesure de concevoir et de déployer des opérations complètes pour le compte de tiers. C'est ce qu'a mis en évidence notre rapport Portal Kombat, qui a révélé le rôle d'une entreprise russe domiciliée en Crimée, Tigerweb, dans la gestion de faux sites d'information.

Plus récemment, lors des élections municipales, Viginum a également détecté un nouveau mode opératoire informationnel qui implique une société privée basée en Israël, spécialisée dans la vente de prestations d'opérations de déstabilisation en ligne. Ce prestataire a mis en place un réseau de plusieurs noms de domaine et de comptes sur les réseaux sociaux et a visé à en particulier le parti LFI, ainsi que plusieurs de ses candidats. Cependant, les éléments techniques obtenus n'ont pas permis d'identifier les éventuels commanditaires de ces opérations en source ouverte, ni leur origine géographique. Enfin, cette opération a bénéficié d'une faible visibilité.

Ces phénomènes illustrent la professionnalisation croissante de l'écosystème des ingérences numériques étrangères, qui se caractérisent désormais par des opérations plus furtives et plus structurées.

Le troisième fait saillant connaît un développement exponentiel depuis un an. Il concerne la prolifération des ingérences numériques étrangères à vocation lucrative. Ce phénomène avait particulièrement été mis en lumière en décembre 2025, avec la diffusion sur Facebook et sur TikTok d'une vidéo générée par intelligence artificielle. Mise en ligne par un jeune Burkinabé et mettant en scène un prétendu coup d'État en France, cette vidéo a fait plus de 17 millions de vues. En vérité cette vidéo visait à faire la promotion des services de ce jeune Burkinabé pour la création de vidéos générées par IA crédibles et authentiques.

Cet exemple illustre un phénomène bien plus vaste, que l'on peut qualifier de systémique, et qui est lié au modèle économique des plateformes. Aujourd'hui, la création et

la diffusion de contenus polémiques ou polarisants à destination d'audiences françaises constituent un véritable *business model* pour de nouveaux types d'acteurs étrangers qui génèrent des revenus, notamment par le biais des programmes de monétisation des plateformes.

Plus largement, ce phénomène pose la question du rôle et de la responsabilité des plateformes dans la formation du débat public numérique. En réalité, par leurs algorithmes, par leur modèle économique, par leurs solutions de monétisation, ces plateformes ont la capacité de façonner notre débat public numérique, en visant un public ciblé et en définissant les conditions d'accès. Nous assistons ainsi à une véritable marchandisation de notre débat public numérique, qui peut générer des risques de sécurité nationale et de déstabilisation démocratique.

J'ajouterai enfin que ces trois tendances saillantes – persistance, professionnalisation des intermédiaires et ingérence numérique étrangère à vocation lucrative – ont été observées par Viginum dans le cadre des élections municipales. Notre secrétaire général Nicolas Roche vous d'ailleurs avait rendu compte de l'expérience du réseau de coordination et protection des élections (RCPE) lors des municipales.

Face à cette menace informationnelle, la France s'est dotée de moyens d'agir, dans le cadre d'une gouvernance interministérielle, qui mène des actions de réponse et vise à imposer collectivement un coût à nos adversaires. Au sein de l'État français, trois domaines se sont structurés dans le champ informationnel autour de ces sujets.

Le premier domaine est le domaine offensif, celui de la lutte informationnelle ou la lutte informatique d'influence. Dotée d'une doctrine depuis 2021, elle est pilotée par le ministère des Armées. L'objectif consiste ici à mettre en place une dialectique avec l'adversaire dans le champ informationnel, de mener des actions en appui d'opérations militaires de nos armées.

Le deuxième domaine est celui de l'influence, dont le chef de file est le ministère de l'Europe et des affaires étrangères. Et enfin le champ défensif est celui de Viginum et du SGDSN, dont l'objectif porte sur la protection du débat public numérique national contre les ingérences numériques étrangères.

Le modèle de Viginum est un modèle quasiment unique au monde, pour lequel la France a été précurseur. Nous sommes un service technique et opérationnel d'investigation en ligne, qui est résolument engagé pour la protection du débat public numérique et qui opère dans un cadre juridique strict, dans le cadre d'un État de droit.

Notre mission a pour objet de détecter et de caractériser ces ingérences numériques étrangères. Nous traitons donc d'une menace spécifique, qui est définie par quatre critères : un critère d'extranéité (l'implication directe ou indirecte d'un acteur étranger, qu'il soit étatique ou non étatique) ; un critère de contenu (contenu manifestement inexact ou trompeur) ; un critère de comportement (caractérisation des procédés techniques mis en œuvre pour une diffusion artificielle ou automatisée, massive et délibérée) et enfin un critère de gravité, puisque nous ne traitons que de la menace qui vise à porter atteinte aux intérêts fondamentaux de la nation.

Nous travaillons uniquement sur les contenus qui sont publiquement accessibles sur les interfaces en ligne. Par ailleurs notre activité est suivie par un comité éthique et scientifique indépendant, chargé de veiller à la conformité de nos travaux avec notre cadre juridique. Celui-ci publie dorénavant chaque année un rapport pour offrir toute la transparence nécessaire sur notre action et notre méthode de travail.

Ainsi, Viginum met en œuvre une approche technique qui s'appuie sur le critère objectif et prend finalement assez peu en compte les contenus et les narratifs. Il s'agit ainsi de caractériser les infrastructures qui ont conduit à la mise en place de ces opérations, à leurs comportements, à leurs techniques et leurs procédés de diffusion. Les narratifs nous intéressent finalement assez peu, puisque nous considérons qu'il ne nous revient pas, en tant que service de l'État, de définir ce qui est vrai ou faux. Notre approche, technique et technologique, est donc centrée sur les acteurs de cette menace et non sur les contenus. Elle nous permet une action plus proactive et une réponse plus stratégique.

Deuxièmement, il ne relève pas des attributions de Viginum de surveiller le comportement d'acteurs français qui mèneraient des actions de manipulation de l'information : nous nous intéressons uniquement aux manœuvres informationnelles étrangères qui visent à porter atteinte à la souveraineté de notre débat public national.

Viginum et ses partenaires interministériels disposent d'une gamme de réponses, que je qualifierais de « défenses actives », face aux ingérences numériques étrangères. La réponse la plus visible concerne ainsi la dénonciation publique ou par canaux diplomatiques des acteurs de cette menace. En collaboration avec le ministère de l'Europe et des affaires étrangères, la France a ainsi dévoilé à plusieurs reprises des ingérences numériques étrangères qui avaient été caractérisées par Viginum ; par exemple, en publiant des rapports techniques sur des actions menées par des modes opératoires informationnels prorusses ou azerbaïdjanais.

Ces révélations visent à porter un coup à nos adversaires, en dévoilant leurs infrastructures, mais également à sensibiliser le public afin d'accroître notre capacité à résister. Ces rapports peuvent par ailleurs contribuer à la mise sous sanction d'individus ou d'entités.

Un autre moyen d'action consiste à essayer de gêner nos adversaires, dans le déploiement de leurs infrastructures. À cette fin, nous coopérons avec les plateformes en ligne : nous pouvons procéder à des signalements techniques, notamment en lien avec la création de faux comptes, de comptes automatisés, laquelle contrevient aux conditions générales d'utilisation des plateformes. En conséquence, elles peuvent entreprendre des actions de modération.

Par ailleurs, nous renforçons nos actions avec l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom), la Commission européenne et la DG Connect, en documentant et en suivant la mise en œuvre du règlement sur les services numériques (DSA), notamment les mesures d'atténuation des risques systémiques en matière de manipulation de l'information.

Enfin, s'agissant des enjeux à venir, il nous semble évident que nous devons collectivement nous préparer à faire face à un durcissement de la menace informationnelle qui n'a jamais été aussi diffuse et donc potentiellement dangereuse pour nos démocraties. Face à

cette réalité, nous sommes convaincus que la réponse régalienne ne suffit pas ; notre résilience collective doit reposer sur une vigilance accrue des citoyens et de l'ensemble des composantes de la nation.

Telle est donc précisément l'ambition de la Stratégie nationale de lutte contre les manipulations de l'information d'origine étrangère qui a été publiée en février 2026, dans le cadre d'un travail collectif pour lequel vous avez également abondamment contribué, aux côtés d'experts, de chercheurs, de membres de la société civile. Ce document fondateur fixe un cadre d'action clair et durable en partant d'une conviction simple : la société elle-même constitue le premier rempart contre la manipulation de l'information.

Nous assisterons le SGDSN dans l'opérationnalisation de cette stratégie. Nous étant vus confier en février 2026 une mission d'information du public, nous porterons un certain nombre d'initiatives, que je pourrai davantage détailler lors des questions-réponses.

M. Loïc Kervran, président. Je vous remercie pour la présentation de la réalité de la menace. Je cède à présent la parole aux orateurs de groupe.

Mme Nadine Lechon (RN). Avant toute chose, je souhaite, au nom de mon groupe, saluer le travail réalisé par le Quai d'Orsay et Viginum. Vous luttez avec pertinence contre les ingérences étrangères. Votre action permet de disposer d'informations transparentes et claires qui sont à la base du fonctionnement de notre démocratie. Cela est d'autant plus nécessaire, à l'heure où les puissances rivalisent de moyens de déstabilisation, que ce soit sur des segments stratégiques, économiques ou réputationnels.

Aussi, permettez-moi d'aller à l'essentiel sur ce qui fâche : une nouvelle ingérence de la Commission européenne dans ce domaine régalien – qui ne révèle pas de sa compétence –, à la fois par le Digital Service Act, mais aussi et surtout par le « bouclier démocratique européen ».

Le Rassemblement national ne laissera pas faire cette démarche fédéraliste, qui est inutile, voire dangereuse. Les différents services de renseignement de l'Union coopèrent déjà ensemble – cela est heureux, car indispensable. Mais n'oublions pas que les alliés peuvent être aussi des compétiteurs, et même des rivaux. Je rappelle à ce titre qu'un ancien président de la République et un ancien ministre des affaires étrangères ont été écoutés par des services allemands, pour le compte de l'administration américaine.

Il est donc hors de question que la Commission vienne rajouter son grain de sel dans ce domaine. Elle y est incompétente, en droit comme dans les faits. Durant plus d'une décennie, la Hongrie de Viktor Orban, démocratiquement et régulièrement élu, a été la cible de tentatives de lutte informationnelle de la Commission, au motif que son gouvernement n'adhérait pas à sa doxa. En matière d'ingérence, Mme von der Leyen maîtrise parfaitement le sujet. Sur le fond, comme sur la forme, la lutte contre les ingérences doit demeurer dans le périmètre de l'État. Madame, monsieur, si jamais le bouclier démocratique européen devait être adopté, quels seraient les garde-fous concernant la souveraineté, pour ce domaine essentiel qu'est la guerre hybride ?

Mme Anne-Sophie Dhiver. Aujourd'hui, nous travaillons à l'échelle européenne sur ces sujets, qui concernent l'ensemble des démocraties. Depuis environ un an, cette dynamique s'est structurée avec la mise en place d'un véritable bouclier démocratique

européen, incarné notamment par la création d'un centre européen pour la résilience démocratique.

Il convient toutefois de clarifier précisément sa vocation. Ce centre n'a pas pour objectif de devenir un « Viginum européen ». La position de la France a été constante et fermement affirmée sur ce point, considérant qu'il ne saurait disposer de compétences opérationnelles. En particulier, il ne doit en aucun cas être amené à suivre le débat public national, ni à collecter des données le concernant. Le champ des ingérences numériques étrangères et de la protection du débat public relève en effet d'une compétence fondamentalement régalienne, indissociable de la souveraineté nationale.

Pour autant, l'échelon européen demeure indispensable. Son rôle s'exerce d'abord au niveau de la coopération. La lutte contre les ingérences numériques étrangères concerne aujourd'hui l'ensemble des démocraties européennes. De nombreux États ont structuré, ou sont en train de structurer des capacités comparables à celles de Viginum. Or, ce domaine constitue un champ technique encore relativement récent, à l'image de la cybersécurité il y a une quinzaine d'années.

Dans ce contexte, il est nécessaire de structurer une coopération européenne permettant le partage d'analyses, de bonnes pratiques, d'outils et de méthodes. L'objectif est d'élaborer une grammaire commune pour caractériser la menace et faciliter les échanges entre États, afin d'accroître notre interopérabilité et notre capacité à agir de manière coordonnée. La France s'implique pleinement dans ces travaux, aux côtés du ministère de l'Europe et des affaires étrangères et du Secrétariat général des affaires européennes (SGAE), notamment en pilotant un groupe de travail dédié à la standardisation et à la définition de méthodologies.

Par ailleurs, l'échelon européen est également déterminant en matière de régulation. La mise en œuvre du DSA constitue un levier essentiel pour lutter contre la manipulation de l'information et les ingérences numériques étrangères. À cet égard, un travail étroit est conduit avec l'Arcom, la Commission européenne et la DG Connect, afin de garantir une application plus rapide et plus efficace de ce cadre.

Mme Constance Le Grip (EPR). L'audition d'aujourd'hui intervient à un moment charnière dans le contexte de guerre hybride auquel la France doit faire face, comme les autres démocraties européennes. Il faut également relever le cadre de l'évolution très nette de notre doctrine, de notre stratégie de lutte contre les ingérences informationnelles.

Depuis le début de l'année 2026, un véritable changement d'échelle est en cours. En témoignent la publication de la première stratégie nationale de lutte contre les manipulations de l'information, l'élargissement des capacités de Viginum, la mise en œuvre du DSA, la discussion au sein du Conseil et du Parlement européen du bouclier démocratique européen, l'évolution de la posture du Quai d'Orsay, son implication de plus en plus forte dans la bataille informationnelle, et bien sûr, le retour d'expérience des élections municipales.

Nous ne faisons plus face uniquement à des campagnes de désinformation ponctuelles aussi toxiques soient-elles, mais à la mise en place d'infrastructures informationnelles malveillantes, persistantes, permanentes. Dans ce cadre, le travail remarquable des fonctionnaires qui travaillent pour le compte *French Response* doit être salué. Comment le défi de l'intelligence artificielle peut-il être appréhendé de la manière la plus opérationnelle et la plus efficace possible ?

M. Emmanuel Lebrun-Damiens. L'intelligence artificielle constitue à la fois un défi et un levier essentiel d'action. Elle s'impose comme un élément structurant de notre réponse face à l'évolution rapide des menaces. Dans ce cadre, nous utilisons déjà des outils d'écoute sociale qui s'apparentent à des solutions d'intelligence artificielle. Ces logiciels sont paramétrés à partir de mots-clés afin de détecter des signaux faibles, d'identifier des attaques ou des campagnes de désinformation et de permettre une réaction la plus rapide possible.

À ce stade, l'intelligence artificielle est principalement mobilisée dans les fonctions de veille et de détection de la menace. L'objectif est clair : réduire notre temps de réaction et tenter de progresser au même rythme que nos adversaires, voire de le devancer. À cet égard, une accélération notable a été observée en 2026. La crise iranienne constitue un exemple particulièrement marquant. L'utilisation par l'Iran de l'intelligence artificielle pour produire et diffuser des vidéos à fort potentiel viral a été d'une rapidité et d'une efficacité remarquables. Ces contenus ont contribué à structurer un récit stratégique, avec un impact significatif sur les perceptions.

Dans ce contexte, l'intelligence artificielle pose également des défis majeurs en matière de formation et de recrutement. Il est impératif de développer les compétences nécessaires pour maîtriser ces outils. Les grandes puissances se sont déjà engagées résolument dans cette voie, et il est indispensable que nous soyons au rendez-vous de ces évolutions technologiques.

Mme Anne-Sophie Dhiver. En complément, il convient de souligner que l'intelligence artificielle constitue effectivement un double enjeu, à la fois un levier opérationnel et un risque systémique. Du point de vue des usages observés par Viginum, force est de constater que la plupart des modes opératoires informationnels actuels recourent désormais à l'intelligence artificielle générative. Celle-ci est mobilisée pour produire, à grande échelle, des contenus variés, qu'il s'agisse d'articles longs, d'images, de vidéos ou encore de commentaires ciblés en direction d'audiences très spécifiques. Ces contenus ne relèvent pas nécessairement du *deepfake* au sens strict, mais visent souvent à renforcer la charge émotionnelle, afin de susciter un fort engagement du public et inciter ce dernier à les relayer.

Ce recours massif à la génération automatisée constitue déjà une évolution significative, mais d'autres transformations, encore plus préoccupantes, peuvent être anticipées. Aujourd'hui, une part croissante de la population, estimée à 20 % des Français selon certaines études, utilise régulièrement des outils conversationnels fondés sur l'intelligence artificielle pour s'informer. Dans ce contexte, il existe une hypothèse selon laquelle ces agents conversationnels pourraient être instrumentalisés pour diffuser des narratifs d'origine étrangère.

À ce stade, les manœuvres dites de « *LLM grooming* », consistant à tenter d'influencer les modèles de langage par une diffusion massive de contenus biaisés, demeurent relativement limitées et exigeraient des efforts importants de la part des acteurs malveillants. En revanche, deux évolutions suscitent davantage d'inquiétude. La première tient à la possibilité de manipulations « en boîte blanche » des algorithmes, comme l'illustrent certaines modifications régulières observées dans des systèmes tels que Grok, susceptibles d'orienter les résultats ou de promouvoir certains narratifs.

La seconde concerne l'émergence de l'intelligence artificielle agentique. Celle-ci pourrait donner naissance à des agents autonomes pilotés par IA capables de produire, publier et interagir de manière crédible, rendant leur détection particulièrement difficile.

À ce stade, ces évolutions constituent davantage une transformation progressive qu'une rupture immédiate. Parallèlement, l'intelligence artificielle demeure un outil essentiel pour Viginum. Elle permet de traiter des volumes de données qui dépassent largement les capacités humaines, notamment en automatisant certaines analyses. Des outils ont déjà été développés et mis en ligne, notamment en open source, pour détecter des campagnes massives de contenus générés par IA, dont des manœuvres d'*astroturfing*. Enfin, la création en 2026 d'un centre d'excellence en IA au sein de Viginum vise à renforcer ces capacités en lien avec le monde académique et scientifique.

M. Aurélien Saintoul (LFI-NFP). Je vous remercie pour votre présentation, intellectuellement stimulante et exhaustive. Nous sommes entrés dans une ère d'industrialisation de la propagande, dans laquelle nous entendons l'écho des écrits de Guy Debord. Retournant la dialectique hégélienne, il disait ainsi que le faux n'était plus un moment du vrai, mais que le vrai était un moment du faux. C'est assez saisissant.

Les logiciels dont vous disposez sont-ils pleinement souverains ? Ma deuxième question porte sur l'analyse des algorithmes. Disposez-vous d'un accès suffisant aux algorithmes des grandes plateformes ? Ensuite, existe-t-il une relation bien établie entre cybermalveillance, fuite de données, manipulation et ingérence ?

Ma quatrième question porte sur les modèles économiques des plateformes. Vous avez dit qu'il fallait maximiser l'engagement. Mais en réalité, le véritable problème n'est-il pas simplement que le modèle économique des plateformes conduit à ce genre de situation ? Ne faudra-t-il pas trancher dans le vif et renoncer à ces modèles économiques pour promouvoir une véritable écologie de l'attention ? Enfin, une évolution législative est-elle nécessaire, selon vous, aujourd'hui ?

M. Emmanuel Lebrun-Damiens. L'outil logiciel que j'ai mentionné concernant la veille est complètement souverain. Ensuite, un certain nombre de vos questions concernent les enjeux essentiels de régulation des plateformes, mais ces sujets ne sont pas suivis par ma direction. De plus, le modèle économique des plateformes constitue un outil extrêmement puissant, notamment ce qui concerne l'utilisation de la publicité à des fins géopolitiques, la manière dont ce canal peut être utilisé par des adversaires.

Mme Anne-Sophie Dhiver. Dans le cadre de nos missions d'investigation, nous utilisons à Viginum trois principales catégories outils. La première regroupe des solutions commerciales, telles que les outils de *social listening*, qui permettent de suivre les dynamiques sur les réseaux sociaux et d'identifier des écosystèmes de comptes ou des modes opératoires informationnels, au quotidien. Aucun outil ne couvrant à lui seul l'ensemble des plateformes avec une profondeur suffisante, plusieurs solutions sont utilisées conjointement.

La deuxième catégorie comprend des outils *open source*, notamment des modèles d'intelligence artificielle, qui servent de base à des développements spécifiques. Enfin, la troisième catégorie correspond aux outils développés en interne, adaptés à des cas d'usage précis, comme l'analyse à grande échelle des contenus textuels.

Ces outils sont soit *open source*, soit d'origine française ou européenne, afin de répondre aux exigences de souveraineté. Toutefois, l'essentiel ne réside pas dans la technologie elle-même, mais dans l'expertise humaine. L'analyse repose sur la capacité des agents à identifier des indices pertinents et à reconstituer des chaînes d'information. Le renseignement d'origine sources ouvertes (Osint) ne se réduit pas à une logique de *big data*, mais exige une compréhension fine des contextes.

Enfin, il est évident que l'architecture algorithmique des plateformes, leur modèle économique, façonne la hiérarchie des contenus et le débat public numérique. Notre relation avec les plateformes repose sur une coopération technique, parfois perfectible. Lorsque celle-ci se révèle insuffisante, les mécanismes prévus par le règlement européen sur les services numériques (DSA) offrent des leviers d'action, qui doivent permettre d'engager une action efficace. Par ailleurs, sur le plan national, nous pouvons être conduits à collaborer ou à être mandatés par les autorités judiciaires.

M. Thierry Sother (SOC). Vous l'avez rappelé, la France s'est dotée d'objectifs ambitieux. Nous sommes passés d'une notion de riposte à une notion de contre-récit. Dans le plan présenté le 7 mai par le ministère de l'Europe et des affaires étrangères, plusieurs moyens forts ont été annoncés, tels que la création d'un contingent dédié à la guerre informationnelle ou encore l'identification de trente zones de guerre informationnelles.

Cette volonté coïncide également avec les ambitions fortes affichées pour Viginum – service jeune, mais dont l'utilité est saluée sur quasiment tous les bords de notre Assemblée –, telles que mentionnées dans la stratégie nationale de lutte contre les manipulations de l'information. Je pense notamment à l'Académie portée par Viginum, qui aurait pour triple vocation d'informer le grand public, d'éduquer en lien avec l'éducation nationale et de former les partenaires français et internationaux. En sait-on plus aujourd'hui sur l'échéance de déploiement de cette Académie ?

Aussi, Viginum comptait quarante-deux équivalents temps plein (ETP) en 2025, contre un objectif de soixante-cinq. De même, son budget n'a pas été à la hauteur de ce que souhaitaient les socialistes lors du dernier débat. Considérez-vous que les objectifs affichés par Viginum et par le ministère de l'Europe et des affaires étrangères sont atteignables rapidement ? Les moyens pour y parvenir sont-ils suffisants, considérant le fait que nous entrons maintenant en période d'élection présidentielle et potentiellement législative ?

Enfin, en matière d'ingérence étrangère, notre meilleure protection reste sans aucun doute l'application de normes et en particulier le DSA, comme vous l'avez évoqué à l'instant. S'ils ont été longtemps réclamés, la Commission européenne a commencé à prendre des premières sanctions. En savez-vous aujourd'hui plus sur les avancées des nombreuses enquêtes en cours ? Quelles ambitions peut-on espérer de la part de la Commission européenne sur une véritable application du DSA, qui combine des enquêtes, mais également les sanctions, telles qu'elles sont prévues dans ce document ?

Mme Anne-Sophie Dhiver. L'Académie de la lutte contre les manipulations de l'information de Viginum a été préfigurée depuis plusieurs mois ; elle est d'ores et déjà pleinement mobilisée. Son lancement officiel interviendra en juin, mais ses travaux ont déjà débuté. Une équipe dédiée a été constituée à cet effet, appuyée par des moyens supplémentaires.

Cette académie s'articule autour de trois missions principales. La première consiste à assurer une mission d'information et de sensibilisation du public. Cette mission a été formellement confiée à Viginum dans le cadre de la mise à jour de son décret en février 2026. Dans cette perspective, l'académie permettra d'intensifier la publication de bulletins d'information réguliers, dans la continuité des travaux déjà engagés, notamment à travers les bulletins du RCPE. L'objectif consiste bien à améliorer la compréhension des citoyens et de renforcer leur vigilance face aux opérations de manipulation de l'information.

La deuxième mission porte sur la formation. L'académie a vocation à concevoir et diffuser des contenus de formation à destination de publics variés. Il s'agit à la fois des professionnels, des acteurs de la société civile, des médias, mais également des élèves et de leurs enseignants. L'ambition est de transmettre les savoir-faire, notamment en matière d'investigation en source ouverte, et de structurer une offre de formation cohérente. Des initiatives ont déjà été mises en œuvre, comme des challenges d'investigation, des podcasts et des formations développées en lien avec le Centre de liaison de l'enseignement et des médias d'information (Clemi), accessibles sur la plateforme Magistère. Cette dynamique sera amplifiée.

Enfin, la troisième mission concerne le développement des relations avec le monde académique et scientifique. Il vise à structurer une filière de recherche associant à la fois les disciplines techniques et les sciences humaines et sociales, afin d'approfondir l'analyse des phénomènes liés à la manipulation de l'information.

S'agissant des moyens, Viginum dispose aujourd'hui de soixante-cinq équivalents temps plein. Les renforts obtenus récemment permettent de développer ces nouvelles capacités, notamment l'Académie et le centre d'excellence en intelligence artificielle en cours de préfiguration. Dans ces conditions, les ressources actuelles offrent la capacité de conduire des actions substantielles et structurantes.

M. Emmanuel Lebrun-Damiens. Je reviendrai sur la question des moyens, qui demeure un enjeu central, en donnant des éléments chiffrés permettant d'apprécier l'investissement de nos adversaires dans le champ informationnel. Selon les informations dont nous disposons, la Russie consacre chaque année entre 2 milliards d'euros et 2,6 milliards de dollars à ses opérations de propagande dans le champ informationnel. La Chine mobiliserait quant à elle des montants bien supérieurs, de l'ordre de 48 milliards de dollars. L'Iran s'inscrirait à un niveau intermédiaire, avec environ 1,8 milliard de dollars, tandis que le seul département de la guerre américain alloue environ 1,2 milliard de dollars à ses propres productions. Ces chiffres illustrent le caractère extrêmement coûteux et stratégique de ces actions.

Face à de tels volumes d'investissement, nous déployons l'ensemble des programmes possibles, en fonction des moyens dont nous disposons. La direction de la communication publique a ainsi bénéficié d'une augmentation de ses ressources, à la suite d'une décision ministérielle validée par la représentation nationale, ainsi que de redéploiements internes. Néanmoins, ces moyens demeurent limités au regard des capacités adverses.

À titre indicatif, le budget de la DCP s'élève aujourd'hui à 16 millions d'euros, comme en attestent les documents budgétaires. Des créations d'emplois ont également été

réalisées jusqu'à l'été 2025. Parallèlement, nous appliquons strictement les orientations du premier ministre visant à contenir les dépenses de communication institutionnelle. Toutefois, la guerre informationnelle relève d'un registre distinct, qui impose de prendre pleinement la mesure des investissements et des stratégies de nos adversaires.

Mme Anne-Sophie Dhiver. Aujourd'hui, nous estimons que le DSA constitue un outil d'action globalement efficace, dans la mesure où il couvre l'ensemble des dimensions pertinentes. Toutefois, il apparaît nécessaire d'envisager certaines évolutions, en particulier s'agissant des lignes directrices relatives à l'atténuation des risques systémiques, notamment en période électorale.

Ces lignes directrices, adoptées en 2024, doivent désormais être réexaminées à l'aune de l'évolution rapide de la menace. À cet égard, plusieurs pistes peuvent être envisagées. Il serait ainsi pertinent de réfléchir à un encadrement plus strict des systèmes algorithmiques en période électorale, par exemple à travers un gel temporaire des algorithmes de recommandation ou une meilleure mise en avant renforcée de contenus issus de sources d'information crédibles et légitimes.

Par ailleurs, certains enjeux nécessitent d'être davantage intégrés, tels que la suppression effective des comptes inauthentiques, le marquage clair des contenus générés par intelligence artificielle, ainsi que le respect des obligations en matière de transparence publicitaire. Il conviendrait également de renforcer l'opérationnalisation des dispositions relatives à l'accès aux données pour les chercheurs.

Enfin, une réflexion doit être menée sur la capacité d'action des États membres dans leur champ d'intervention légitime, étant entendu que la protection des processus électoraux demeure une prérogative souveraine.

M. Jean-Louis Thiériot (DR). Je vous remercie pour cet exposé, qui montre combien la guerre informationnelle et la guerre des récits figure au cœur de la résilience de nos sociétés.

Ma première question concerne l'enjeu des *deepfakes*, et notamment des images, films ou vidéos générées par l'IA. La grande difficulté est la suivante : souvent, ce qui est vu est cru. Quel est l'état de vos réflexions pour essayer d'établir un organisme « certificateur » ?

Ensuite, s'agissant de Viginum, vous avez clairement précisé que votre champ d'intervention concernait les cas comportant des éléments d'extranéité. Comment gérer la zone grise entre ces structures et leurs filiales ou associations « sœur » ? Quelle est votre doctrine en la matière ?

Ma dernière question s'adresse plutôt au Quai d'Orsay. Quel *benchmark* ou *mapping* avez-vous réalisé des attaques informationnelles contre nos partenaires de l'UE ? Sommes-nous plus ciblés que d'autres ? Quelle est un peu votre analyse de la situation ?

M. Emmanuel Lebrun-Damiens. Je commencerai par répondre à votre dernière question. Le SGAE publie chaque année un rapport consacré aux attaques numériques étrangères, lequel met en évidence que 90 pays à travers le monde sont aujourd'hui victimes de ce type d'attaques. Dans ce panorama, la France apparaît comme le deuxième pays européen le plus touché, après l'Ukraine. Ce constat n'est pas anodin et s'explique en grande

partie par le positionnement de notre diplomatie, qui porte une voix forte sur les grandes crises internationales, notamment sur le dossier ukrainien, et qui nous expose de ce fait à des opérations hostiles, qu'elles soient authentiques ou inauthentiques.

Face à cette situation, notre réponse s'inscrit résolument dans une logique partenariale. Nous développons des coopérations étroites avec nos partenaires européens, fondées sur l'échange de bonnes pratiques et la recherche d'une efficacité accrue dans nos actions communes.

S'agissant des *deepfakes*, leur capacité de nuisance est particulièrement frappante. Nous avons pu le constater concrètement lors de la conférence des ambassadrices et des ambassadeurs : en quelques minutes, il est possible de produire un discours entièrement falsifié, difficile à distinguer du réel. Cette réalité appelle deux réponses complémentaires. Il s'agit d'une part du développement de capacités de vérification, où le rôle de la société civile est essentiel. Il s'agit d'autre part de consacrer un effort accru d'éducation à l'information, afin d'adopter un nouveau réflexe consistant à questionner systématiquement par défaut la véracité des contenus.

Mme Anne-Sophie Dhiver. S'agissant de l'intelligence artificielle, permettez-moi de compléter en apportant la perspective de Viginum. Vous avez raison de souligner que son usage par les opérateurs de la menace poursuit aujourd'hui trois finalités principales. La première est celle du mensonge, consistant à produire et diffuser des contenus entièrement faux afin de donner une apparence de crédibilité à des événements fictifs ou à des prises de parole inexistantes. La deuxième finalité est celle de l'amplification, qui repose sur la diffusion massive de contenus dupliqués ou légèrement modifiés à un rythme très élevé. La troisième finalité, probablement la plus prégnante, est celle de la persuasion. Dans la majorité des cas observés, l'enjeu n'est pas tant de recourir à des *deepfakes* sophistiqués, qui demeurent encore relativement détectables, que de construire des narratifs plus efficaces en s'appuyant sur des éléments visuels ou textuels générés par l'intelligence artificielle. Ces contenus, en renforçant l'émotion et la crédibilité apparente, suscitent un engagement accru.

La difficulté majeure réside dans le doute généralisé que ces pratiques induisent, en brouillant la frontière entre contenus authentiques et synthétiques. Ce phénomène peut conduire à une perte de confiance globale, y compris à l'égard d'informations véridiques. Par ailleurs, des risques systémiques apparaissent, notamment en matière de biais ou d'orientation des modèles eux-mêmes.

À ce titre, l'un des enjeux de ce centre d'excellence en intelligence artificielle consistera à contribuer au programme d'évaluation et de sécurité de l'IA de l'Institut national pour l'évaluation et la sécurité de l'intelligence artificielle (Inesia), qui œuvre sous l'égide du SGDSN en matière de manipulation de l'information. Nous travaillerons conjointement avec l'Institut national de recherche en sciences et technologies du numérique (Inria). Les capacités adverses évoluent en permanence. Aujourd'hui, il existe des détecteurs de conduits synthétiques, mais ils peuvent rapidement devenir obsolètes.

Votre deuxième question concerne les acteurs et la « zone grise » que vous mentionniez. Notre méthode s'intéresse plutôt à la chaîne haute, enfin à remonter le plus haut possible dans cette chaîne de mise en place de ces opérations ; nous cherchons à identifier le primo diffuseur ; puis le premier compte qui a rediffusé cette opération. Il s'agit ensuite, et

surtout, de remonter la chaîne des intermédiaires et prestataires impliqués, de discerner les infrastructures techniques utilisées. L'objectif consiste à puiser aux racines de ces opérations, pour voir caractériser éventuellement l'implication directe ou indirecte d'un acteur étranger.

M. Damien Girard (EcoS). Depuis le déclenchement de la guerre d'agression russe en Ukraine, le 24 février 2022, la Russie s'est encore davantage isolée des pays occidentaux, ce qui l'a conduite à rechercher de nouveaux partenariats sur la scène internationale, et notamment sur le continent africain.

Ce pivot stratégique vers l'Afrique s'inscrit dans le concept de politique étrangère 2023 de la Fédération de Russie. Cette stratégie ne repose pas uniquement sur les relations entre États ; elle s'appuie également sur une politique d'influence informationnelle de plus en plus structurée, mêlant communication politique, relais médiatiques, réseaux sociaux, opérations d'influence et parfois manipulations coordonnées d'information.

Après la mort d'Evgueni Prigojine en 2023, ce dispositif a connu une réorganisation importante. Plusieurs travaux européens soulignent désormais le rôle d'une plateforme appelée « *African Initiative* », présentée comme une vitrine d'influence liée aux services russes. Celle-ci combine action en ligne et sur le terrain, organisation de conférences, partenariats médiatiques, production de contenus numériques et diffusion de récits politiques centrés sur la dénonciation du néocolonialisme occidental, la promotion d'un prétendu « nouvel ordre mondial » ou encore la valorisation de la coopération russo-africaine.

Ces stratégies prospèrent d'autant plus qu'elles s'appuient sur des fragilités et des ressentiments réels, notamment la défiance envers certaines puissances occidentales ou les crises politiques locales. C'est précisément cette capacité à exploiter des tensions existantes qui rend ces opérations particulièrement efficaces et difficiles à détecter. Un rapport conjoint du Service européen pour l'action extérieure et de Viginum a montré que ces réseaux d'influence actifs en Afrique disposaient également de relais au Royaume-Uni, capables de relayer, amplifier ou coordonner certains narratifs anti-occidentaux au-delà du continent africain.

Les autorités françaises ont-elles identifié l'existence d'écosystèmes comparables sur notre territoire en lien avec African Initiative ou avec d'autres structures d'influence russe ? Si tel est le cas, quels sont aujourd'hui les principaux acteurs ou modes opératoires observés, qu'il s'agit de réseaux numériques, d'événements publics, de relais médiatiques ? Quel niveau de risque ces dispositifs représentent-ils pour notre espace démocratique, nos débats publics, ou la prévention des ingérences étrangères ?

Mme Anne-Sophie Dhiver. Je vous remercie de revenir sur ce rapport. Publié en février 2025, il s'agit du premier rapport réalisé en coopération avec des partenaires internationaux. Il revient sur la recomposition du dispositif d'influence russe en Afrique après la mort d'Evgueni Prigojine. Cette chaîne s'appuie sur un *continuum* d'acteurs, qu'il s'agisse d'acteurs officiels, de pseudo-associations comme *African Initiative*, mais aussi de relais et d'influenceurs pour mettre en œuvre ces procédés.

S'agissant de votre dernière question, le champ d'action de Viginum concerne uniquement les acteurs étrangers. En conséquence, la caractérisation d'éventuels acteurs français ne relève pas de notre domaine.

Mme Josy Poueyto (Dem). Ma première question porte sur le périmètre de vos interventions. La présence d'un acteur étranger est nécessaire à la caractérisation de l'ingérence. L'action indépendante de citoyens français en relais d'acteurs étrangers entre-elle dans le champ de vos compétences ?

La deuxième question concerne le comité d'éthique et scientifique de Viginum, qui constatait dans son rapport d'analyse de l'activité 2024 que l'ingérence numérique étrangère ne disposait pas d'une qualification pénale propre et s'appuyait sur des infractions déjà existantes. Estimez-vous qu'une qualification pénale spécifique serait de nos jours justifiée ?

Par ailleurs, sur la base du code électoral et de la loi relative à la lutte contre la manipulation de l'information, qui prévoit que le juge des référés peut être également saisi pour faire cesser la diffusion d'informations trompeuses de nature à altérer la sincérité du scrutin par le biais d'un service de communication au public en ligne, êtes-vous en capacité d'intervenir en appui technique dans la procédure civile, pour accompagner le juge dans la caractérisation d'une infraction en lien avec une ingérence ?

Mme Anne-Sophie Dhiver. En premier lieu, le critère d'implication d'un acteur étranger est absolument déterminant dans l'action de Viginum. Il constitue, en réalité, la condition essentielle de mise en œuvre de notre mandat tel qu'il est défini par décret. Nous n'intervenons pas sur des opérations qui ne comporteraient pas cette dimension. Notre approche est ainsi strictement centrée sur les acteurs et non sur les contenus eux-mêmes.

Dans cette perspective, notre objectif consiste à remonter le plus haut possible dans la chaîne de diffusion et de mise en œuvre des opérations d'ingérence. Nous cherchons à identifier le primo-diffuseur. Les relais nationaux éventuels ne constituent pas le cœur de notre analyse. Cette approche présente un double avantage. D'une part, elle permet de mieux comprendre et caractériser les infrastructures techniques utilisées. Cela nous donne la capacité d'anticiper certaines actions, par exemple en identifiant en amont la création de nouveaux sites ou de noms de domaine liés à ces infrastructures, parfois avant même leur promotion publique. D'autre part, elle ouvre la voie à une action plus stratégique, en permettant de qualifier l'implication d'acteurs étrangers et de soutenir des démarches de dénonciation publique ou de sanction en lien avec le Quai d'Orsay.

S'agissant du cadre juridique, il convient de rappeler que de nombreux outils existent déjà. Les dispositifs issus de la loi du 22 décembre 2018, notamment le référé dit « anti-fake news », ainsi que certaines dispositions du code électoral, offrent des leviers mobilisables. Leur activation pourrait être encore renforcée. C'est dans cet esprit que le Garde des Sceaux a récemment diffusé aux autorités judiciaires deux circulaires, l'une sur la manipulation de l'information, l'autre sur l'ingérence étrangère.

Des pistes d'amélioration peuvent néanmoins être envisagées dans différents dispositifs législatifs. Par exemple, le champ d'application du référé « anti-fake news » pourrait être élargi à certains scrutins non couverts actuellement. Aujourd'hui, il concerne uniquement les élections nationales ; il ne couvrait pas par exemple les élections municipales. Il ne me revient pas de me prononcer à ce sujet ; il appartiendra à nos autorités politiques de décider si elles veulent formuler des propositions d'évolution législative.

M. Michel Criaud (HOR). Dans un contexte de multiplication des opérations d'ingérence numérique étrangère, la France a fait le choix de se doter d'une stratégie nationale, élaborée sous l'égide du SGDSN. Nous le savons : la France est une cible bien identifiée, privilégiée des ingérences étrangères. La multiplication des vidéos générées par l'intelligence artificielle, de faux comptes relayant aussi des contenus mensongers, et des campagnes de désinformation en période électorale, notamment sur les réseaux sociaux, nous obligent à faire constamment évoluer nos dispositifs, afin de protéger le débat public et garantir un espace informationnel fondé sur la liberté d'expression et la pluralité des opinions.

Créé en 2021, l'objectif de Viginum est de préserver le débat public des manipulations de l'information provenant de l'étranger et sur les plateformes numériques. Comment appréhendez-vous le recours croissant à l'IA dans les ingérences étrangères et quels sont les leviers de riposte de Viginum dans ce domaine ? Deuxièmement, qu'apporte concrètement la nouvelle stratégie de lutte contre les manipulations de l'information adoptée par la France en ce début d'année ?

Mme Anne-Sophie Dhiver. S'agissant de l'intelligence artificielle, j'ai déjà eu l'occasion d'évoquer à plusieurs reprises ses usages actuels par les opérateurs de la menace, qui sont désormais largement généralisés. À ce stade, il s'agit avant tout d'une évolution technologique qui accompagne la menace sans en transformer encore radicalement la sévérité. Toutefois, la rapidité des progrès observés dans ce domaine suscite des préoccupations légitimes quant à l'évolution prochaine des capacités adverses.

Dans ce contexte, nous mobilisons quotidiennement l'intelligence artificielle dans nos activités. Deux défis majeurs se dégagent. Le premier consiste à accélérer encore l'intégration de l'IA dans nos méthodes de travail. L'ampleur des avancées récentes impose de suivre ce rythme et d'intégrer de manière plus systématique ces outils dans l'ensemble de nos processus.

Le second défi réside dans la nécessité d'anticiper et d'évaluer les risques associés à ces technologies, notamment les risques systémiques qu'elles peuvent générer en matière de manipulation de l'information. Ces deux dimensions – le développement de nouveaux cas d'usage et l'analyse des risques – relèveront pleinement des missions du centre d'excellence dédié à l'intelligence artificielle.

Par ailleurs, la stratégie nationale de lutte contre les manipulations de l'information d'origine étrangère constitue un document fondateur. Pour la première fois, un document de stratégie nationale définit un cadre d'action global, articulé autour de quatre priorités et de quinze objectifs stratégiques.

La première priorité porte sur la construction d'une résilience démocratique. Le renforcement de l'immunité collective passe par l'information, la sensibilisation et la formation du public. Notre Académie y contribuera, au même titre que les acteurs de l'éducation ou du monde académique. La deuxième priorité vise à continuer d'encadrer et responsabiliser les plateformes. L'enjeu concerne notamment d'atténuation des risques systémiques de l'usage de leurs services, sur les réseaux sociaux ou les solutions d'IA, notamment d'IA générative. Cela passe notamment par la pleine mise en œuvre des outils disponibles, du DSA au règlement européen sur l'IA.

La troisième priorité concerne le renforcement des capacités régaliennes, impliquant différents acteurs de l'État, notamment Viginum, le Quai d'Orsay, le ministère de l'intérieur, le ministère des armées. En fait, de renforcer au niveau capacitaire dépend notre capacité à détecter, caractériser et à répondre à ces opérations. Enfin, la quatrième priorité s'attache à développer la coopération internationale, en particulier à l'échelle européenne, afin de développer des standards, une meilleure capacité collective à analyser cette menace et à y faire face. L'enjeu, désormais, réside dans l'opérationnalisation effective de cette stratégie. Nous serons pleinement impliqués, auprès du SGDSN, dans l'exécution de cette stratégie qui fixe des objectifs concrets et actionnables. Ils nous permettront de donner une direction très claire à l'action de l'État, pour agir sur l'ensemble des enjeux liés à cette menace.

M. Emmanuel Lebrun-Damiens. S'agissant de la mise en œuvre de la stratégie de lutte contre les manipulations de l'information, je souhaiterais insister sur un point essentiel et, en l'occurrence, porteur d'une note positive. Nous observons aujourd'hui une amélioration réelle de la résilience de la société française, comme en attestent plusieurs sondages.

Trois facteurs principaux permettent d'éclairer ces différences. Le premier tient aux cadres de régulation, qui varient d'un pays à l'autre. Le deuxième facteur réside dans les usages. Dans certains pays, la presse intermédiée conserve une place centrale, contribuant à structurer l'accès à l'information et à limiter l'exposition à des contenus manipulés. À l'inverse, dans d'autres contextes, la consommation repose davantage sur les réseaux sociaux, qu'il s'agisse de circuits « ouverts » comme sur X, TikTok ou Facebook, ou d'espaces plus fermés comme les messageries de type WhatsApp ou Signal, où la circulation de l'information est moins transparente et plus difficile à appréhender. Enfin, le troisième facteur est précisément celui de la résilience. Au même titre que la France, de nombreux pays investissent ce champ, à juste titre.

M. Loïc Kervran, président. Nous passons maintenant à une séquence de deux questions individuelles complémentaires.

M. José Gonzalez (RN). Le débat public sur les ingérences numériques se concentre souvent, et à très juste titre, sur les grandes puissances comme la Russie, la Chine ou les États-Unis. Mais l'actualité récente montre aussi la capacité de puissances régionales ou intermédiaires à mener des stratégies beaucoup plus diffuses, parfois en s'appuyant sur des relais médiatiques, religieux, culturels ou des diasporas présentes sur le territoire. On l'a vu à différentes occasions autour des tensions du Proche-Orient ou des fréquentes campagnes d'influence turque ou algérienne dans plusieurs pays européens.

Comment appréhendez-vous le potentiel de relais de certains éléments de ces diasporas ? Bien entendu, il ne s'agit pas de stigmatiser toutes les personnes qui composent ces diasporas, notamment dans notre environnement numérique. Enfin, notre doctrine de lutte contre les ingérences est-elle vraiment adaptée à ces stratégies plus diffuses, parfois même moins prises au sérieux que les opérations classiques attribuées aux grandes puissances ?

M. Aurélien Saintoul (LFI-NFP). Quelle est la relation entre cybermalveillance et manipulation ? Les fuites de données constituent-elles un levier, un moyen pour manipuler ? Ensuite, vous avez évoqué la tentative d'ingérence qui a visé notamment les candidats de LFI, en précisant qu'aujourd'hui, il était toujours impossible de définir quels

étaient le ou les éventuels commanditaires. Est-il envisageable, à brève ou à moyenne échéance, de parvenir à attribuer ce genre d'attaques ? Quelles perspectives proposez-vous, quels sont les axes de progression ?

M. Emmanuel Lebrun-Damiens. S'agissant de la distinction entre grandes puissances et puissances régionales ou intermédiaires, je tiens à préciser que, dans nos outils de réponse comme dans les récits que nous produisons, nous ne faisons aucune différenciation. Notre action ne poursuit aucun objectif politique. Nous sommes « agnostiques » sur le choix des attaques auxquelles nous répondons et dans la réponse que nous apportons. Nous répondons à ceux qui nous attaquent, quelle que soit la taille du pays, quelle que soit leur puissance.

S'agissant, de la question des diasporas, notre réponse est claire : notre champ d'intervention se situe exclusivement à l'échelle du champ informationnel mondial, en dehors du territoire national. Dans ce contexte, les diasporas peuvent naturellement être concernées, mais uniquement dans leur dimension extérieure. Ainsi, lors d'un événement tel que le sommet Africa Forward, notre communication s'adresse à l'opinion publique africaine, mais également à l'opinion publique internationale dans son ensemble. Les diasporas africaines, présentes à l'échelle mondiale, s'inscrivent dans ce public élargi et peuvent être légitimement destinataires de cette communication, dès lors qu'elles se situent hors de France.

Mme Anne-Sophie Dhiver. Il est fréquent de rapprocher la menace cyber de la menace d'ingérence d'origine étrangère. Cette association n'est pas dénuée de fondement. Il existe en effet des zones de recoupement. Certains acteurs peuvent adopter des stratégies duales, opérant simultanément sur le terrain cyber et dans le champ informationnel. L'exemple des « Macron Leaks » en 2017 illustre ce type d'articulation. Par ailleurs, certaines opérations d'ingérence empruntent des procédés issus de la cybercriminalité, tels que le *typosquatting* ou l'usurpation d'identité de sites internet. Dans ces cas, des coopérations sont naturellement engagées, notamment avec l'Agence nationale de la sécurité des systèmes d'information (Anssi), au sein du SGDSN, afin de traiter les interfaces entre ces deux formes de menaces.

Toutefois, la menace d'ingérence étrangère demeure distincte par nature. Elle touche directement aux questions d'information, de perception et de débat public. Elle ne saurait être réduite à une problématique purement technique, que ce soit dans sa détection, sa caractérisation ou son traitement. Le modèle de Viginum repose sur cette spécificité, à savoir un cadre éthique et juridique garantissant à la fois l'efficacité opérationnelle et le respect des droits et libertés fondamentaux.

S'agissant des opérations récemment documentées dans le cadre du réseau de coordination et de protection des élections, il convient de rappeler que Viginum n'agit pas isolément. Son action s'inscrit dans une gouvernance interministérielle, structurée autour du comité opérationnel de lutte contre les manipulations de l'information (Colmi), qui permet le partage d'éléments techniques avec différents partenaires. Viginum assure la détection, la caractérisation et une partie de l'imputation technique, puisque nous travaillons en source ouverte.

L'attribution ne relève pas de notre ressort. En revanche, dans le cadre de nos travaux interministériels, nous partageons l'ensemble des éléments sur les différentes

opérations que nous détectons à nos partenaires, notamment les services de renseignement, qui disposent d'autres moyens que les nôtres pour procéder à cette attribution.

Enfin, j'ajoute que nous sommes en cours de finalisation d'un rapport qui sera rendu public et contiendra l'ensemble des éléments dont nous disposons. Il reviendra non seulement sur l'action du RCPE, mais aussi sur les détails techniques de ces opérations.

M. Loïc Kervran, président. Je vous remercie.

La séance est levée à douze heures trente-sept.

*

* *

Membres présents ou excusés

Présents. - Mme Caroline Colombier, M. Michel Criaud, Mme Geneviève Darrieussecq, Mme Alma Dufour, Mme Sophie Errante, M. Yannick Favennec-Bécot, M. Thomas Gassilloud, M. Damien Girard, M. José Gonzalez, M. Laurent Jacobelli, M. Loïc Kervran, Mme Nadine Lechon, Mme Josy Poueyto, M. Aurélien Saintoul, M. Thierry Sother, M. Jean-Louis Thiériot, M. Romain Tonussi

Excusés. - Mme Valérie Bazin-Malgras, M. Christophe Blanchet, Mme Anne-Laure Blin, M. Frédéric Boccaletti, M. Manuel Bompard, M. Hubert Brigand, Mme Blandine Brocard, M. Charles Fournier, M. Moerani Frébault, Mme Catherine Hervieu, M. Pascal Jenft, M. Bastien Lachaud, M. Antoine Léaument, Mme Lise Magnier, Mme Alexandra Martin (Alpes-Maritimes), Mme Anna Pic, Mme Isabelle Rauch, M. Arnaud Saint-Martin, Mme Isabelle Santiago, M. Mikaele Seo, M. Boris Vallaud, M. Laurent Wauquiez

Assistait également à la réunion. – Mme Constance Le Grip