ASSEMBLÉE NATIONALE

17e LÉGISLATURE

Mercredi
25 mars 2026
Séance de 9 heures

Compte rendu n° 40

SESSION ORDINAIRE DE 2025-2026

Compte rendu

Commission de la défense nationale et des forces armées

– Audition, ouverte à la presse, de M. Nicolas Roche, Secrétaire général de la défense et de la sécurité nationale, sur la stratégie nationale de lutte contre les manipulations de l'information 2

– Information relative à la commission 25

Présidence de M. Jean-Michel Jacques, *Président*

ASSEMBLÉE NATIONALE

La séance est ouverte à neuf heures cinq.

M. le président Jean-Michel Jacques. Mes chers collègues, permettez-moi tout d'abord de rendre hommage au major Arnaud Frion du 7e bataillon de chasseurs alpins, mort pour la France en Irak dans l'accomplissement de sa mission. Dans le cadre de la lutte contre le terrorisme, il a été frappé par une attaque de drones, aux côtés de plusieurs de ses frères d'armes qui ont été blessés et à qui nous souhaitons un prompt rétablissement. Le major était une figure, un sous-officier remarquable, qui avait reçu plusieurs citations et médailles militaires. Il a également été décoré de la Légion d'honneur, à titre posthume. Nous assurons à sa famille et à ses camarades tout notre soutien et nous nous tenons à leurs côtés.

Nous accueillons aujourd'hui Monsieur Nicolas Roche, secrétaire général de la défense et de la sécurité nationale. La lutte contre les ingérences étrangères et la désinformation, en particulier dans le champ du numérique, constitue un enjeu essentiel pour la France et pour l'Europe ; à plus forte raison, en période électorale. De telles attaques hostiles dans notre pays, comme chez nos partenaires européens, n'ont pas manqué ces derniers mois et se reproduiront très certainement.

Le secrétariat général de la défense et de la sécurité nationale (SGDSN) que vous dirigez, monsieur le secrétaire général, joue un rôle fondamental en la matière. Je rappelle que vous travaillez aussi avec Viginum, dont vous avez la charge. Vous avez ainsi élaboré récemment une stratégie nationale de lutte contre les manipulations de l'information (LMI) pour la période 2026-2030. À ce titre, vous avez bien voulu faire contribuer les parlementaires, ce dont je vous remercie. Vous aviez déjà utilisé cette méthode dans le cadre de la revue nationale stratégique (RNS) ; je considère qu'elle est réellement remarquable.

Sans plus tarder, je vous cède la parole.

M. Nicolas Roche, secrétaire général de la défense et de la sécurité nationale, sur la stratégie nationale de lutte contre les manipulations de l'information. Mesdames et Messieurs les députés, j'ai plaisir à être devant vous ce matin pour évoquer le sujet spécifique de la stratégie de lutte contre les manipulations de l'information d'origine étrangère, que nous avons publiée en février dernier à l'issue d'un long processus. Je suis accompagné ce matin par Jean Cattan, le principal coordonnateur de l'élaboration de cette stratégie, qui pourra compléter mon propos sur quelques éléments plus spécifiques.

Mon propos se concentrera sur les enjeux de notre nation face à cette stratégie hybride de manipulation de l'information et du rôle particulier que le SGDSN joue dans ce cadre, qu'il s'agisse du pilotage de Viginum ou de son rôle de coordination interministérielle.

En 2025, le SGDSN a coordonné un travail d'actualisation de nos grandes stratégies et de notre réflexion stratégique. Il s'agit naturellement de la RNS, à laquelle votre commission a puissamment contribué, mais il faut également mentionner la stratégie nationale spatiale publiée en novembre dernier, la stratégie nationale de cybersécurité, ou encore la publication du guide « *Tous responsables* » figurant au cœur de notre stratégie nationale de résilience et qui a été publié à l'occasion du congrès des maires de France. Il convient en outre de souligner la première feuille de route du travail de l'Institut national pour l'évaluation et la sécurité de l'intelligence artificielle (Inesia), ainsi que la grande stratégie nationale de lutte contre les manipulations de l'information, que nous avons publiée

le 11 février dernier. Désormais, depuis l'été dernier, l'enjeu principal concerne la mise en œuvre opérationnelle de ces grandes réflexions stratégiques, afin qu'elles guident l'action de l'ensemble de l'État, des administrations centrales et territoriales.

S'agissant de la lutte contre les manipulations de l'information, je souhaite formuler cinq remarques. La première porte sur la définition de la menace. Je ne reviens pas sur ce texte, auquel vous avez là aussi beaucoup contribué. Nous avons fait le choix, dans l'introduction, d'essayer de clarifier les termes et de produire un véritable effort de définition. La désinformation, les manipulations de l'information, les *fake news*, les ingérences numériques étrangères constituent des concepts parfois utilisés de façon un peu indiscriminée, et la confusion provient parfois de notre propre mauvais emploi des termes, y compris au sein de l'administration. Cet effort de définition nous a conduits à recentrer notre propos autour des manipulations de l'information d'origine étrangère, autrement dit, pour le traduire en termes juridiques, des ingérences numériques étrangères (INE).

En conséquence, je concentrerai spécifiquement mon propos sur cette question des ingérences numériques étrangères, tout en reconnaissant qu'elles n'épuisent pas la totalité du champ des enjeux informationnels qui nous sont posés. Ces ingérences numériques étrangères sont définies par quatre critères qui définissent notre compétence et qui figurent dans le décret de création de Viginum. Il y a d'abord un critère d'extranéité, autrement dit nous ne nous intéressons qu'aux acteurs étrangers, étatiques ou non étatiques, impliqués dans ces attaques informationnelles. Deuxièmement, il existe effectivement, mais il n'est pas majeur, un critère de contenu, puisqu'il s'agit de contenus manifestement inexacts ou trompeurs. Mais surtout, les deux critères essentiels sont, d'une part, un critère technique, celui de l'amplification inauthentique de l'ensemble des contenus par des méthodes massives et délibérées, et, d'autre part, un critère de gravité, puisque ces attaques informationnelles doivent être de nature à porter atteinte aux intérêts fondamentaux de la nation. Ainsi, tout ce qui se déroule dans le champ informationnel n'est pas, par construction, de nature à porter atteinte aux intérêts fondamentaux de la nation tels qu'ils sont définis dans notre droit positif.

Tel est le cœur même de l'objet « ingérences numériques étrangères » ou « manipulation de l'information d'origine étrangère » dont je souhaite vous entretenir ce matin. Lorsque l'on observe les dernières années, nous constatons une évolution de la menace des ingérences numériques étrangères qui est à la fois préoccupante et significative, autour de trois éléments, trois critères ou trois paramètres. Le premier est un paramètre de nature stratégique. Nous constatons aujourd'hui que nos grands adversaires, les grands acteurs des manipulations de l'information d'origine étrangère, s'inscrivent dans une logique de persistance stratégique. Autrement dit, il existe une continuité dans l'action de ces acteurs qui, tous les jours, en permanence, en période électorale comme en dehors de toute période électorale, conduisent des opérations d'ingérence numérique étrangère. Ils le font avec une volonté très claire de s'ingérer, au sens précis et technique du terme, dans notre débat numérique afin de l'influencer, en se faisant passer pour des acteurs français, ce qui constitue précisément le cœur de l'ingérence. Cette persistance des acteurs stratégiques représente un élément fondamental de notre appréciation actuelle de la menace telle qu'elle pèse sur notre débat numérique et sur notre démocratie.

Il existe, évidemment, un certain nombre d'acteurs plus spécifiquement prégnants dans ces opérations d'ingérence numérique étrangère ou de manipulation de l'information d'origine étrangère. Naturellement, nous pensons tous à la Russie, mais nous avons

également – et nous l'avons rendu public – détecté un certain nombre d'opérations d'une nature différente en provenance du territoire chinois, ainsi que d'Iran. Il existe également un sujet autour de certaines sphères étrangères, y compris des acteurs non étatiques de la sphère MAGA, qui conduisent de façon persistante des opérations d'ingérence numérique étrangère visant à s'implanter durablement dans notre débat numérique.

La deuxième caractéristique de l'évolution de la menace est de nature technologique. Les mutations technologiques auxquelles nous sommes confrontés transforment profondément notre paysage informationnel. Le paramètre technologique le plus spontanément mentionné concerne l'utilisation croissante de l'intelligence artificielle (IA). On y pense souvent à travers ce qui touche le plus directement les citoyens et les consommateurs d'information, en particulier sur les plateformes, c'est-à-dire la génération de contenus synthétiques par l'intelligence artificielle, ce que l'on appelle dans un vocabulaire anglicisé, les *deepfakes*. Pour être très honnête, ces contenus ne sont pas si difficiles que cela à détecter. Le véritable enjeu de l'utilisation de l'intelligence artificielle dans les opérations de manipulation de l'information et d'ingérence numérique étrangère est beaucoup plus profond et concerne la manipulation des modèles d'IA eux-mêmes.

Au-delà de cette question, il existe une mutation globale du paysage technologique, liée à l'importance croissante des plateformes numériques dans l'économie de l'information et dans l'économie de l'attention, ainsi qu'à la prégnance des modèles algorithmiques de hiérarchisation des contenus. À cette dimension s'ajoute évidemment celle de l'intelligence artificielle. Ce paysage technologique en évolution rapide et profonde engendre un impact direct, dans la mesure où il fournit autant d'outils technologiques à la disposition de ceux qui souhaitent s'ingérer dans notre débat numérique et qui utilisent ces moyens technologiques avancés pour conduire leurs opérations d'ingérence numérique étrangère.

Le troisième paramètre de l'évolution de la menace est encore plus large et touche à la transformation globale de notre écosystème informationnel. Il concerne l'évolution de la production de l'information, le passage des médias traditionnels vers les plateformes numériques, mais aussi l'émergence de nouveaux acteurs, notamment les influenceurs, qui peuvent aujourd'hui être des acteurs de la manipulation de l'information, volontairement ou involontairement. Dans cette économie de l'attention, il est également possible, et nous y avons été confrontés récemment, que certaines opérations d'ingérence numérique étrangère poursuivent une finalité strictement lucrative. Ces opérations n'ont pas nécessairement d'objectif politique ou stratégique, mais exploitent les mécanismes de monétisation des plateformes et des réseaux sociaux, où le fait de générer des clics, de la polarisation et du débat permet de générer des revenus.

Ces nouveaux acteurs, qu'il s'agisse des plateformes numériques, des influenceurs ou d'acteurs privés utilisant des opérations d'ingérence numérique étrangère à des fins lucratives, participent à l'évolution de notre environnement informationnel et transforment la menace. Cette triple évolution stratégique, technologique et économique constitue une réalité constatée ces dernières années, appelée à durer. Elle confirme que le pari collectif fait avec la création de Viginum en 2021 était empreint de clairvoyance, puisque la menace que nous observons aujourd'hui est massive, permanente et persistante, en période électorale comme en dehors.

Mon deuxième point vise précisément à dresser un point d'étape sur le principal instrument dont l'État s'est doté depuis près de cinq ans pour la détection et la caractérisation des opérations d'ingérence numérique étrangère : Viginum, le service de vigilance sur les ingérences numériques étrangères, rattaché directement au SGDSN et placé sous mon autorité. Ce service a établi, dès sa création, deux choix fondamentaux qui conditionnent son efficacité dans la durée.

Le premier est un choix de nature technique. Viginum se consacre avant tout à la détection et à la caractérisation des infrastructures numériques d'amplification inauthentique. Il s'agit donc d'un service technique et technologique qui s'intéresse moins aux contenus qu'aux infrastructures utilisées par les acteurs des INE pour s'implanter de manière subreptice dans notre débat numérique national. Ce choix est essentiel, à la fois parce que nos adversaires recourent à des méthodes d'anonymisation et à des infrastructures de plus en plus sophistiquées, nécessitant des compétences pointues en investigation numérique, et parce qu'il constitue une condition d'acceptabilité démocratique. Viginum n'est pas un « ministère de la vérité ». Il ne dit pas ce qui est vrai ou faux. Son rôle consiste à préserver la souveraineté française.

Le second choix fondamental consiste à se concentrer exclusivement sur les acteurs étrangers. Les débats entre acteurs français sur les réseaux sociaux ou les plateformes sont politiquement importants, mais ils ne relèvent pas du cœur de mission des responsables de la défense et de la sécurité nationale. Viginum se concentre sur les acteurs étrangers, étatiques ou non étatiques, et sur les modes opératoires informationnels par lesquels ils s'ingèrent dans notre débat numérique en se faisant passer pour des acteurs internes.

Ce modèle, relativement spécifique en Europe, a été précurseur. Aujourd'hui, face à une menace qui touche l'ensemble de nos partenaires, chacun d'entre eux se dote de dispositifs similaires selon ses traditions institutionnelles. Certains les rattachent aux ministères des affaires étrangères, d'autres aux services de renseignement. Nous avons opéré le choix d'un service interministériel, technique, tourné vers l'étranger, transparent, soumis au contrôle d'un comité éthique et scientifique et de la Commission nationale de l'informatique et des libertés (Cnil), et ne travaillant qu'à partir d'informations ouvertes. De fait, Viginum n'a jamais été pensé comme un service de renseignement.

Autour de ce service, une comitologie interministérielle a été mise en place, notamment avec le ministère de l'Europe et des affaires étrangères, qui a renforcé ses capacités en matière de narratif et de communication stratégique, en particulier à travers « French Response ». Après cinq ans d'activité, nous avons révisé le cadre juridique de Viginum en fusionnant les deux décrets de 2021. Ce nouveau décret, adopté en février après avis favorable de la Cnil et du Conseil d'État, conserve les fondements du modèle tout en l'adaptant à l'évolution technologique.

En premier lieu, l'ensemble des éléments fondamentaux du modèle de Viginum demeurent, c'est-à-dire que nous n'avons pas touché au cadre et aux éléments fondamentaux, Nous avons cependant choisi de les adapter à l'évolution de la menace technologique. En 2021, le seuil de collecte des données autorisées par la CNIL à Viginum avait été fixé à cinq millions d'utilisateurs par jour, qui nous permettait de collecter des données publiques sur les grandes plateformes, qui engendrent un effet systémique sur notre débat numérique. Or, par expérience, nous avons constaté qu'une partie des opérations d'INE que nous sommes

conduits à détecter commencent en réalité sur des plateformes plus petites, dans des environnements numériques bien plus restreints, plus clos.

Nous avons donc supprimé le seuil de cinq millions d'utilisateurs uniques par mois afin de pouvoir collecter des données sur des plateformes plus petites et détecter au plus tôt la survenue d'une opération d'INE. Nous avons également allongé les durées de conservation des données afin de mieux comprendre les infrastructures persistantes (réseaux de *bots*, chaînes d'anonymisation, faux sites web) utilisées par les acteurs malveillants. Ces évolutions renforcent notre capacité d'anticipation tout en renforçant la transparence et le contrôle démocratique. Nous avons par ailleurs renforcé les prérogatives et les compétences du comité éthique et scientifique, l'obligation de transparence de Viginum, et donc, *in fine*, votre contrôle parlementaire et celui de nos concitoyens.

En résumé, ce décret révisé, publié au *Journal officiel* le 12 février dernier, nous donne les moyens dont nous estimions avoir besoin pour continuer notre mission de détection, de caractérisation et de gêne des acteurs de la menace informationnelle.

Le troisième point concerne la surveillance des élections municipales. Nous avons mis en place un dispositif spécifique dès janvier, partant du principe que les acteurs de la menace informationnelle restent actifs en période électorale. Cette hypothèse a été confirmée par les faits. Nous avons également mené des consultations approfondies avec les commissions compétentes et les groupes politiques, diffusé un guide d'information aux candidats et assuré une communication régulière et transparente.

Ensuite, le principe de régularité et de transparence, principe cardinal de notre dispositif de protection des élections, a effectivement été mis en œuvre, puisque dix bulletins d'information ont été publiés chaque semaine depuis février sur le site du SGDSN. Nous élaborons actuellement un bilan, que nous publierons dans le cadre d'un rapport final. Celui-ci établira un retour complet sur les événements intervenus et mettra en lumière les enseignements qui en ont été retirés.

Nous avons détecté au moins quatre grandes opérations d'ingérence numérique étrangère. Ces opérations ont eu très peu d'impact et très peu de visibilité, mais elles ont démontré de manière très claire la volonté d'un certain nombre d'acteurs de peser sur notre débat. Elles illustrent, une nouvelle fois, le caractère permanent et intentionnel de ces tentatives d'ingérence, même lorsque leurs effets concrets demeurent limités.

Les deux derniers points que je vais aborder plus rapidement portent sur les suites que nous avons tirées de ces constats. Nous avons également réfléchi, et c'est un élément de transition vers la stratégie elle-même de lutte contre les manipulations de l'information, à la question du droit et à la question de l'utilisation du droit comme outil de protection et de prévention face aux opérations d'ingérence numérique étrangère. Je pense ici au droit électoral, au droit pénal et, potentiellement, au droit civil, mobilisés comme des armes juridiques pour nous prémunir contre ces menaces.

Comme vous le savez, nous avons inscrit cette réflexion dans la stratégie nationale de lutte contre les manipulations de l'information qui a été publiée en février. Deux circulaires du garde des Sceaux ont été publiées, l'une sur la question générale des ingérences, l'autre sur la question des manipulations de l'information. Elles ont rappelé à l'ensemble des acteurs du monde judiciaire l'intégralité des dispositions juridiques existantes dans nos codes,

notamment le code pénal, le code électoral et le code civil, qui peuvent être mobilisées par la justice pour lutter contre les opérations de manipulation de l'information et d'ingérence numérique étrangère. Nous disposons d'ores et déjà d'un dispositif juridique étoffé, profond, et qui pourrait être utilisé de manière plus utile et plus agressive que ce que nous faisons aujourd'hui.

Nous avons néanmoins identifié certaines pistes d'amélioration. En 2018, votre Assemblée, le Parlement, a adopté une loi que l'on appelle communément la « loi anti *fake news* » en période électorale, qui correspond aujourd'hui à l'article L 163-2 du code électoral. Le choix opéré à l'époque, et qui était probablement conforme à l'état de la menace en 2018, limite toutefois le recours au juge civil en référé aux seules élections nationales. Ce dispositif ne permet donc pas son application aux élections locales. Concrètement, cela signifie que cet article n'aurait pas pu être employé durant les élections municipales, ou toute autre élection locale. Ce type de limitation nous conduira probablement à revenir vers vous afin de suggérer certaines évolutions du droit, pour continuer à adapter notre droit électoral, pénal ou civil à l'évolution de la menace. Par ailleurs, l'article L. 97 pourrait également mériter quelques modifications. Cela pourrait nous conduire, dans les mois à venir, à vous proposer des ajustements ciblés de notre droit.

Le dernier point concerne la stratégie nationale de lutte contre les manipulations de l'information d'origine étrangère, que nous avons rassemblée dans un document publié en février. S'agissant de la méthode, au sein de l'État, nous sommes sans doute les premiers à avoir conscience que la lutte contre les manipulations de l'information ne peut pas être uniquement l'affaire de l'État, et encore moins celle du seul État central. Il s'agit d'une affaire qui doit embarquer l'intégralité de la nation.

C'est pour cette raison que nous avons choisi une méthode d'élaboration de la stratégie nationale de lutte contre les manipulations de l'information la plus participative possible. Nous l'avons évidemment réalisé en lien avec les commissions compétentes de la défense et de la culture des deux assemblées. Surtout, nous avons voulu lancer, avec l'organisation Make.org, une vaste consultation publique citoyenne qui a rencontré un fort succès, puisqu'elle a recueilli plus de 10 000 contributions. Nous avons ainsi souhaité fédérer et intégrer les idées issues de la société civile, tout en consultant largement les acteurs du monde de l'information et de la lutte contre les manipulations de l'information.

Cette stratégie engage l'État, puisqu'elle a été rédigée et coordonnée par l'État, mais nous avons voulu qu'elle soit le fruit d'une véritable co-construction. L'engouement et la qualité des contributions, y compris les vôtres, que nous avons intégralement prises en compte, en témoignent.

Enfin, le second élément sur lequel j'insisterai concerne le pilier de la résilience de la nation. En effet, si les dispositifs de Viginum, la protection des élections, le droit et les moyens d'entrave relèvent principalement de l'action de l'État, nous avons la conviction très forte que l'immunité collective face aux opérations d'ingérence numérique étrangère et de manipulation de l'information suppose que l'ensemble de nos compatriotes soient informés et résilients. C'est pourquoi nous engageons un vaste travail de pédagogie, d'information et d'éveil à destination des collectivités territoriales, des acteurs économiques, de la société civile et de nos concitoyens. Nous allons par exemple créer une Académie de lutte contre les

manipulations de l'information, afin que chacun puisse devenir une partie de la réponse à cette menace croissante.

M. le président Jean-Michel Jacques. Je vous remercie pour ce propos très nourri et très précis. Je cède à présent la parole aux orateurs de groupe.

Mme Michèle Martinez (RN). Monsieur le Secrétaire général, je tiens à saluer les 600 cyber-combattants qui ont été engagés sur l'opération Orion 2026, dans le cadre de la lutte d'influence. De fait, la bataille cognitive et narrative cohabite avec les opérations classiques engageant nos forces. Une fausse information peut produire un effet stratégique en quelques heures. Dans ce contexte, je remercie, au nom du groupe RN, le SGDSN pour son travail encore peu documenté sur la manipulation de l'information.

Le bon fonctionnement de la démocratie repose sur un accès à l'information aussi ouvert et fiable que possible. Nos ennemis, comme nos compétiteurs, ont identifié ce levier d'information comme une faille dans nos sociétés. Nous agréons à la plupart des points de votre rapport. Aussi, permettez-moi d'aller directement à l'essentiel et ainsi d'évoquer les sujets qui fâchent. J'ai noté à de nombreuses reprises dans votre rapport une volonté d'accroître les pouvoirs de la Commission européenne.

Or la défense et la sécurité relèvent par essence de la responsabilité de la nation qui les protège. La Commission européenne n'est en aucun cas qualifiée pour s'ingérer dans la lutte contre la manipulation de l'information. La proposition visant à assurer dans le cadre européen la capacité d'action des autorités en période électorale n'est donc pas acceptable. La France dispose d'une communauté de renseignement efficace, à laquelle le RN renouvelle sa confiance.

Les services de renseignement partagent des informations et des bonnes pratiques avec leurs homologues européens. Il s'agit là d'une réalité qui conditionne déjà leur efficacité. Je rappelle d'ailleurs que, bien qu'alliés, ces services ne partagent pas toujours les mêmes intérêts. Quoi qu'il en soit, le fait qu'une institution non élue par le peuple français soit chargée d'assurer la sécurité de ses élections constitue une atteinte à la sécurité que ne permettent ni la Constitution, ni les traités. Notre groupe rejette donc des objectifs stratégiques visant à bâtir un bouclier démocratique européen. Il existe déjà un juge des élections en France, le Conseil constitutionnel.

Monsieur le secrétaire général, j'aimerais entendre vos précisions sur ces éléments. En aucun cas, la lutte légitime contre les manipulations de l'information ne saurait se traduire par une nouvelle ingérence de la Commission dans un domaine qui n'est absolument pas le sien.

M. Nicolas Roche. Ma réponse se concentrera exclusivement sur la dimension technique. Je ne rentrerai pas dans des débats politiques, car tel n'est pas mon rôle. Sur la partie technique, il me semble utile d'apporter quelques précisions importantes sur l'articulation entre le niveau national et le niveau européen. Cette articulation mérite d'être clarifiée.

En premier lieu, il n'existe pas de Viginum européen et il n'y en aura pas. Il existe au niveau européen la création d'un dispositif destiné à permettre la diffusion des bonnes pratiques et à renforcer la coopération entre États membres. En revanche, la dimension

opérationnelle demeure strictement nationale, notamment la capacité technique d'investigation numérique. Cela étant, nous avons besoin, comme vous l'avez vous-même souligné, de renforcer notre « interopérabilité » entre pays européens, c'est-à-dire notre capacité à parler le même langage, à utiliser les mêmes concepts, à échanger de l'information et à nous assister mutuellement en période opérationnelle.

C'est précisément à ce niveau que la dimension européenne apporte une valeur ajoutée réelle, mais cette valeur ajoutée ne concerne pas le cœur opérationnel de l'action de Viginum. Aujourd'hui, cette dimension opérationnelle, qui repose sur l'investigation numérique, reste pleinement nationale. Il convient donc d'aller plus loin dans l'analyse de cette articulation et de distinguer clairement ce qui relève du niveau opérationnel, qui restera national, et ce qui relève des échanges de bonnes pratiques, de la collaboration et de la coopération, pour lesquels des dispositifs européens peuvent être utiles.

Le deuxième point de cette distinction concerne le droit. Vous avez parfaitement raison de souligner que la stratégie nationale de lutte contre les manipulations de l'information d'origine étrangère nécessite l'appui de l'Union européenne. Nous avons en effet besoin de sa puissance normative. Sans commenter les dimensions politiques de votre intervention, je rappelle par exemple que la régulation des plateformes relève aujourd'hui en grande partie du règlement sur les services numériques (DSA). Le DSA est un règlement européen que la France a fortement soutenu et qui contient des dispositions extrêmement utiles pour réguler l'action des plateformes étrangères sur notre territoire, notamment en période électorale.

Le DSA impose en particulier aux très grandes plateformes la limitation des « risques systémiques », prévue à l'article 35. Or, il est évident que certaines plateformes présentent des risques systémiques accrus, notamment en période électorale. À ce titre, le DSA prévoit une obligation de transparence algorithmique, plus théorique que pratique à ce stade. Nous avons besoin, en tant que services de l'État, de savoir si les grandes plateformes modifient leurs algorithmes avant ou pendant les élections. Cette exigence de transparence ne peut être satisfaite que par le droit européen et par la mise en œuvre effective du DSA.

Nous avons donc besoin du règlement européen et de l'action de la Commission européenne pour imposer ces obligations aux plateformes de manière plus offensive et pour renforcer l'exécution du DSA, en particulier de son article 35. À ce stade, la mise en œuvre reste incomplète et nous ne disposons pas d'une transparence parfaite sur l'évolution des modèles algorithmiques en période électorale. C'est pourquoi l'action de l'Union européenne est non seulement utile, mais indispensable, sur ce point.

Mme Natalia Pouzyreff (EPR). Monsieur le secrétaire général, c'est avec un grand intérêt que le groupe Ensemble pour la République a pris part à la consultation de notre commission dans l'élaboration de la stratégie nationale de lutte contre les manipulations de l'information. Nous nous sommes appuyés notamment sur les travaux que nous avions menés avec Marie Récalde dans le cadre d'une mission d'information dédiée à ce sujet, dont nous avons remis le rapport en juillet dernier.

Afin de poursuivre le dialogue fructueux que nous avons conduit avec le SGDSN, je me permets de revenir sur quelques-unes de nos recommandations. D'abord, concernant la coordination des acteurs, la stratégie prévoit que le comité opérationnel de lutte contre les

manipulations de l'information (Colmi) soit transformé en plateforme de coordination opérationnelle dans une configuration plus permanente, mais aussi la mise en place de canaux d'échange pour améliorer la circulation de l'information avec les acteurs concernés. Qu'en est-il d'élargir au cas par cas des ministères non régaliens comme le ministère de l'enseignement supérieur, pour susciter peut-être des formations ? Je rappelle que la semaine actuelle est dédiée à l'éducation aux médias, au sein de l'éducation nationale.

Ensuite, s'agissant de la logique d'amplification de la riposte, « French Response » a su créer un engagement. Dans cet esprit, il nous paraissait intéressant de nous appuyer sur des profils spécialisés en stratégie de communication sur les différents réseaux sociaux ou plateformes. Vous avez fait référence à des influenceurs précédemment, je souhaiterais connaître votre réaction sur ce point.

Troisièmement, la stratégie de lutte contre les manipulations de l'information fixe un objectif de structuration de l'écosystème pour renforcer la résilience de la nation, notamment à travers la création d'une académie portée par Viginum, le soutien à la recherche en sciences cognitives ou en associant la communauté OSINT. Pouvez-vous esquisser les modalités de déclination concrètes et un calendrier pour cet objectif stratégique ?

Enfin, nous proposions dans notre rapport d'information la création de référents, élus ou parlementaires, au sein de l'Académie, à même d'alerter le Parlement et de répondre aux demandes d'information. Qu'en pensez-vous ?

M. Nicolas Roche. Je fournirai, ici aussi, des remarques de nature technique. Il existe une différence très claire, dans l'ensemble des éléments de comitologie et dans la mise en œuvre de la stratégie, entre ce qui relève du niveau technique et ce qui relève du niveau de la coordination des différentes politiques publiques qui concourent à la LMI. À titre, le Colmi Tech est centré sur les capacités des acteurs qui nous aident à conduire l'investigation numérique. En effet, tous les acteurs interministériels ne disposent pas des compétences et de l'expertise nécessaires pour mener une investigation numérique au sens plein du terme, c'est-à-dire repérer des marqueurs, pivoter, rechercher des chaînes d'anonymisation, les dévoiler, conduire des recherches en source ouverte. De telles compétences très techniques, relativement de niche, exigent une expertise spécifique. C'est précisément cet objectif que nous poursuivons à travers la permanence et l'opérationnalisation du Colmi Tech, qui constitue une organisation et un pilotage de la communauté des experts techniques au sein de l'État, indispensables à la conduite de nos investigations numériques.

Cette démarche est assez différente de celle qui relève de la comitologie, laquelle est liée à la mise en œuvre de la stratégie nationale de lutte contre les manipulations de l'information, et en particulier de son premier pilier consacré à la résilience. Cette comitologie a vocation à embarquer l'ensemble des ministères. Nous serons d'ailleurs conduits, dans les semaines qui viennent, à en préciser plus finement les modalités. Nous avons veillé à réunir autour de la table la totalité des ministères concernés, et parmi ceux dont l'engagement est absolument indispensable et qui sont très fortement mobilisés à nos côtés, figurent évidemment le ministère de l'éducation nationale, le ministère de l'enseignement supérieur et de la recherche, mais aussi, par exemple, le ministère de l'agriculture pour la question de l'enseignement agricole.

S’agissant plus spécifiquement de l’animation de cet écosystème, l’Académie de lutte contre les manipulations de l’information, pilotée par Viginum, constitue clairement un chantier pour 2026. Comme je le disais initialement, notre ambition ne consiste pas à rédiger des stratégies, mais à les mettre en œuvre maintenant, tant nous partageons tous un sentiment d’urgence très profond. Cette Académie est en cours de préfiguration et sera mise en œuvre dans le courant de l’année 2026. Nous disposons des moyens nécessaires pour le faire en interne et nous allons les redistribuer en conséquence.

Enfin, sur votre dernier point relatif à la stratégie de communication ou « *strat com* », il s’agit d’un sujet qui relève avant tout du ministère de l’Europe et des affaires étrangères. Je souhaite néanmoins rappeler qu’une stratégie efficace de réponse aux ingérences numériques étrangères suppose la mobilisation de l’ensemble des instruments dont nous disposons : instruments techniques, instruments judiciaires et juridiques, instruments de communication publique, instruments de sanctions, y compris européennes, et instruments de communication stratégique et de riposte informationnelle. Chaque acteur de l’interministériel a sa part de responsabilité. La *strat com* relève du Quai d’Orsay, qui a profondément renforcé ses capacités, notamment à travers « French Response » et l’action de ses équipes de diplomates et d’experts, lesquelles constituent une part essentielle de la réponse collective.

Je cède la parole à Jean Cattan, qui évoquera l’animation de l’écosystème.

M. Jean Cattan, secrétaire général du Conseil national de l’intelligence artificielle et du numérique. Un très grand travail a effectivement été accompli au cours de l’élaboration de cette stratégie, notamment grâce à la réunion de ces entités interministérielles, quels que soient leurs environnements, du plus au moins régalien.

Ces formats, où se trouvaient réunis dans une même pièce le ministère de la Culture, les services de renseignement et l’Éducation nationale, montraient très clairement la force et la puissance de cette dynamique collective que nous avons essayé de retranscrire dans l’écrit, mais qui était déjà présente dans le processus d’élaboration.

Je peux témoigner également de cette capacité propre au SGDSN à mobiliser l’ensemble de l’État, ce qui est particulièrement puissant. Enfin, je veux souligner l’existence du réseau des hauts fonctionnaires à la défense et à la sécurité dans chaque ministère, qui constitue un point d’ancrage et permet une opérationnalisation immédiate de la coordination interministérielle. Il s’agit là de très grands atouts pour assurer la cohésion de l’action de l’État.

M. Arnaud Saint-Martin (LFI-NFP). Monsieur le secrétaire général, nous tenons tout d’abord à saluer le travail de prévention que vous avez mené aux côtés des groupes politiques, et qui visait à expliquer, pour mieux les parer, les mécanismes d’ingérence numérique étrangère à l’œuvre pendant les périodes électorales. Néanmoins, des ingérences ont perturbé ce scrutin. La Russie a, nous le savons, créé de nombreux faux sites simulant la presse française, notamment afin de favoriser le RN et des candidats d’extrême droite.

Des campagnes d’affichage mensongères et diffamatoires ont également visé nos candidats insoumis à Toulouse, à Roubaix et à Marseille. On apprend par ailleurs dans la presse que ces raids numériques auraient été menés par des sociétés situées en Israël, qui utilisent toutes les possibilités offertes par les plateformes pour injecter et faire proliférer leurs

contenus toxiques. Les réseaux sociaux numériques constituent en effet un théâtre de ces opérations de manipulation.

Je citerai aussi Mme Sarah Knafo, candidate Reconquête à Paris, qui a par exemple vu sa visibilité sur X fortement amplifiée par les logiques algorithmiques de la plateforme, quand d'autres candidats ont essuyé au même moment des campagnes de dénigrement et de *trolling* à échelle industrielle ou ont été invisibilisés dans ce cloaque informationnel.

Ces constats obligent le gouvernement à agir à l'approche de l'élection présidentielle. Il est impératif de garantir le bon déroulement du scrutin. La principale préoccupation demeure le rôle des grandes plateformes. En effet, ces systèmes sont entre les mains d'une poignée d'oligarques états-uniens, dont l'objectif est de brutaliser la société par une idéologie suprémaciste et néofasciste. Depuis la réélection de Donald Trump, les garde-fous ont disparu. La réponse de la France et de l'Union européenne est insuffisante ; le DSA ne change pas la donne de façon significative. Il faudra pourtant instaurer un véritable rapport de force avec ces acteurs étrangers, bien décidés à forcer l'alignement des démocraties du Vieux Continent sur leur agenda d'extrême droite.

Dans ce contexte propice au *collapse* démocratique, la stratégie adoptée par le Brésil, qui a menacé ces plateformes de les suspendre si elles ne fournissaient pas des garanties claires quant à la transparence des algorithmes et la régulation des contenus illégaux, peut-elle, selon vous, constituer une solution opérationnelle efficace pour la France et sa souveraineté électorale, alors même que la campagne présidentielle commence bientôt ?

M. Nicolas Roche. Une nouvelle fois, j'aborderai plusieurs points, essentiellement techniques, afin de me cantonner strictement à mon rôle de fonctionnaire. Premièrement, je considère qu'aujourd'hui, l'état du droit européen existant, et en particulier le DSA, son article 35 et l'obligation d'atténuation des risques systémiques qui y est prévue, pose un véritable sujet quant à l'effectivité de sa mise en œuvre. Si l'on prend des enjeux aussi centraux que la transparence algorithmique ou l'obligation de retrait des comptes inauthentiques, pour ne citer que ces deux exemples, force est de constater que le cadre juridique existe, mais que sa traduction concrète demeure insuffisante.

Des avancées positives ont toutefois été réalisées récemment. Les mises en demeure adressées par la Commission européenne à plusieurs grands acteurs des plateformes numériques constituent un premier signal encourageant. Par ailleurs, des prises de position publiques et politiques fortes ont eu lieu ces dernières semaines, au plus haut niveau de l'État, à commencer par le président de la République. Néanmoins, il est nécessaire d'aller beaucoup plus loin et de manière beaucoup plus active dans la mise en œuvre du droit européen existant. Nous disposons, pour être parfaitement honnêtes, d'un certain nombre d'idées techniques sur la façon d'interpréter ce droit à court terme de manière plus agressive, afin de garantir son effectivité et d'assurer que les grandes plateformes numériques respectent pleinement les obligations qui découlent de notre modèle républicain et démocratique, ainsi que de la préservation de notre souveraineté.

Deuxièmement, nous étions initialement incertains lorsque nous avons engagé ce travail collectif avec l'ensemble des groupes politiques et des commissions, autour des principes qui ont fondé notre action collective. Ces principes d'information préalable, de

transparence, de publication régulière, d'anticipation et de caractère routinier étaient directement inspirés de l'expérience de plusieurs de nos partenaires, notamment européens et canadiens. Nous ne savions pas précisément ce que cela produirait dans le contexte politique spécifique d'une campagne électorale en France en 2026. Il est d'ailleurs important de souligner que nous ne sommes pas encore au terme de cette démarche.

Nous allons tirer les enseignements de ce qui s'est produit. À titre personnel, je considère que notre action collective constitue plutôt un succès. Nous avons été capables de détecter et de caractériser des opérations, d'informer les groupes politiques et les candidats, mais aussi de porter une information publique et transparente à destination des électeurs et des citoyens, en temps réel et en anticipation, sans générer de « sur-accidents » ni de « sur-crises ». Ce modèle mérite désormais une réflexion collective afin de déterminer ce que nous souhaitons en faire à l'avenir. Cette réflexion est en cours au sein de l'administration et du gouvernement, et je ne suis pas en mesure, à ce stade, de vous en livrer les conclusions. Cependant, nous avions déjà indiqué que le dispositif mis en place pour les élections municipales constituait également une préparation collective à la séquence électorale de 2027. Il nous appartient désormais d'en tirer les conséquences ensemble.

Le troisième élément qui nous a particulièrement marqués, au SGDSN et à Viginum, tient au fait que nous avons effectivement détecté des opérations d'ingérence numérique étrangère. Nous les avons caractérisées et rendues publiques, tout en poursuivant des investigations qui sont encore en cours. Cette situation nous a parfois conduits à adopter une posture de prudence, car lorsque l'État s'exprime publiquement, il doit être absolument certain de ce qu'il avance. Lorsque ce n'est pas le cas, nous poursuivons les investigations. Nous espérons que les travaux en cours permettront, dans le rapport final attendu en avril, d'aller plus loin, car l'un des enjeux réside dans le décalage entre le temps de la campagne électorale et celui de l'investigation numérique.

Nous avions identifié cette difficulté dès le départ et nous savions qu'elle serait complexe à gérer. Je pense néanmoins que nous l'avons plutôt bien maîtrisée pendant la campagne. Il nous reste maintenant à achever les investigations afin de présenter un rapport complet aux élus et aux électeurs. Je constate néanmoins que les opérations détectées, parfois basiques, mais parfois assez sophistiquées, ont engendré un impact très faible. Les outils d'entrave ont été globalement efficaces et la visibilité de ces opérations dans le débat numérique est restée limitée.

Il ne nous revient pas de porter un jugement, spécifiquement pendant une campagne électorale, sur ce critère juridique qui concerne l'altération manifeste de la sincérité du scrutin. Cet objet relève du juge de l'élection, qui le constate *a posteriori* au regard du droit, de la jurisprudence et d'une série de paramètres qui ne sont pas les nôtres. En revanche, nous savons caractériser le degré de visibilité, à l'aide de métriques plus ou moins sophistiquées. Or en la matière, la visibilité dans le débat numérique de ces opérations d'ingérence numérique étrangère a été finalement assez faible. Le rapport « coût-bénéfice » pour nos adversaires n'a pas été favorable, ce qui constitue une bonne nouvelle pour notre capacité collective à protéger notre souveraineté électorale.

M. Thierry Sother (SOC). À l'heure de l'hybridation des conflits, les tentatives de déstabilisation des démocraties ne sont plus des occurrences ; elles sont devenues systématiques.

En conséquence, se doter d'une stratégie de lutte contre les manipulations de l'information est effectivement essentiel. Poursuivre l'effort en faveur d'une démocratie mieux protégée l'est tout autant. Sur bien des points, le groupe socialiste partage les orientations présentées ici. Premièrement, la stratégie ainsi proposée repose dans une large mesure sur Viginum, un service de pointe essentiel et envié dans le monde, dont nous devons en être fiers. À ce titre, le groupe socialiste a demandé lors du précédent budget des moyens supplémentaires, précisément pour renforcer les équipes de détection et de prévention auprès de la population. Quels sont les moyens supplémentaires que vous envisagez pour Viginum afin d'assurer le renforcement de ses missions et l'exécution de nouvelles missions comme l'académie de lutte contre la manipulation de l'information ?

Ensuite, le deuxième support de cette stratégie repose sur la régulation des plateformes. La semaine dernière, le président de la République a appelé à la Commission européenne à utiliser efficacement le DSA et a revendiqué le droit d'un pays d'agir lui-même dans certaines circonstances. Malheureusement, s'il se perçoit, ce volontarisme n'est pas assez lisible. La Commission européenne commence à activer les sanctions, mais elles interviennent parfois plusieurs années après les faits et certaines irrégularités demeurent inchangées, dans le domaine de la transparence algorithmique.

Quelles actions concrètes et immédiates la France est-elle prête à engager pour nous permettre de réagir rapidement si un algorithme venait à être modifié brutalement au profit d'un camp politique ou si, à l'approche d'une élection, on observait une manipulation évidente des systèmes de recommandations à l'égard d'un candidat ou de ses thèmes de campagne ? Que pouvons-nous faire pour mieux appliquer le DSA ? Sur le plan national, quelles sont les initiatives concrètes envisagées à l'approche des présidentielles ? Qu'offrent-elles comme garanties pour nos libertés ?

M. Nicolas Roche. En tant que secrétaire général, je ne peux refuser par principe les appels à l'augmentation des moyens des institutions, des agences et des services placés sous mon autorité. Toutefois, l'honnêteté m'oblige à rappeler que ces moyens ont été renforcés en 2025 et en 2026. S'agissant de la mise en œuvre de la stratégie nationale de lutte contre les manipulations de l'information telle que nous l'avons conçue, j'estime que les moyens alloués en 2025 et en 2026 nous permettent d'être efficaces, opérationnels, concrets et offensifs, ce qui est l'essentiel pour la protection de notre débat numérique.

La question qui se pose aujourd'hui est davantage une question de ressources humaines. Les moyens supplémentaires ont été agréés, consacrés, votés et arbitrés par le Premier ministre, ce qui constitue, à mon sens, un témoignage à la fois de la confiance que vous nous avez accordée, mais aussi de la conscience aiguë du gouvernement, et du président de la République avec lui, de la priorité absolue que représentent les enjeux de défense et de sécurité nationale, et en particulier la lutte contre les manipulations de l'information.

Le deuxième élément mérite que l'on y revienne. Il concerne le sujet central de la mise en œuvre du DSA. Vous avez rappelé le combat porté par le président de la République auprès de la Commission européenne afin que cette mise en œuvre soit plus rapide, plus offensive, plus efficace et plus massive. Je constate d'ailleurs que ces actions commencent à produire des effets concrets, dans les procédures engagées. Ces procédures ont pu apparaître comme un peu trop lentes et un peu trop timorées, mais il existe incontestablement encore beaucoup de progrès à accomplir.

Il existe ensuite un autre sujet, de nature différente, auquel vous avez fait allusion, et qui concerne le rapport de force. Lorsque l'on pose les termes de l'équation en ces termes, ce rapport de force porte notamment sur des obligations essentielles : la transparence algorithmique, la vérification et la garantie, y compris par des audits algorithmiques rendus possibles, de l'absence de manipulation des algorithmes, l'obligation de retrait de contenus manifestement illégaux, ainsi que l'obligation de retrait de comptes inauthentiques ou d'éléments violant les conditions générales d'utilisation. Sur ces points, nous ne sommes pas encore au bout de ce que nous devons faire.

Pour prendre un exemple très concret, il nous arrive de signaler aux plateformes des comptes inauthentiques, au motif que ces derniers violent leurs propres conditions générales d'utilisation. Mais aujourd'hui, le traitement de ces signalements relève du volontariat des plateformes. Il leur appartient de décider si elles laissent ces comptes prospérer ou si elles les retirent. Or, nous observons que les plateformes sont relativement peu proactives et que leur capacité d'action dépend fortement de leur ligne générale. Dès lors, il apparaît nécessaire de renforcer le droit existant, ou à tout le moins son exécution, en particulier s'agissant des obligations prévues par l'article 35 du DSA.

Pour y répondre efficacement, la manœuvre doit être européenne. Nous serons évidemment beaucoup plus efficaces en agissant au niveau européen, avec nos partenaires, car il s'agit d'une menace qui concerne l'ensemble des États membres. L'exemple roumain, que nous avons tous à l'esprit, illustre chaque jour cette réalité.

Il existe donc de nombreuses actions à mener simultanément. Au niveau national, il s'agit d'exécuter pleinement la stratégie que nous nous sommes donnée. Cela recouvre des dimensions opérationnelles, techniques, des moyens des services de l'État, mais aussi des éléments juridiques. Des modifications du droit seront nécessaires. J'ai déjà mentionné certains articles, comme le L 97 ou le L 163-2, et d'autres dispositions législatives sont à l'étude et pourraient donner lieu à des initiatives sur lesquelles nous serons amenés à revenir vers vous.

Parallèlement, une manœuvre européenne est indispensable. C'est en menant ces deux actions de front, en 2026, que nous pourrons garantir, à la fin de l'année 2026 ou au début de 2027, le dispositif de protection du cycle électoral le plus robuste possible. Évidemment, nous ne serons pas au terme de tout ce qu'il reste à faire à cet horizon. Des travaux, notamment au niveau européen, s'inscriront dans la durée. Mais du côté de l'État, le sentiment d'urgence est réel. Nous allons intensifier notre action tout au long de l'année 2026 sur l'ensemble de nos responsabilités nationales et continuer, sous l'impulsion du président de la République, à être un moteur de l'action européenne pour une mise en œuvre et une interprétation du DSA aussi offensives que possible.

Mme Catherine Hervieu (EcoS). Nous saluons la stratégie nationale de lutte contre les manipulations de l'information, cohérente avec une approche de sécurité globale. Cependant, plusieurs points appellent des clarifications et des renforcements.

S'agissant de la régulation des plateformes, le rôle de l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom) mérite d'être renforcé dans une approche proactive, par exemple, pour détecter les comportements inauthentiques de manière automatisée, massifier les signalements et protéger plus rapidement les victimes. L'idée

d’encoder le droit électoral dans les algorithmes est intéressante, mais imprécise. La France doit clarifier sa doctrine et utiliser pleinement les marges offertes par le droit européen pour protéger l’intégrité démocratique.

Il existe également un angle mort majeur : l’absence de remise en cause du modèle économique dominant des plateformes. Le capitalisme de surveillance fondé sur la publicité et la captation de l’attention constitue un moteur structurel des manipulations de l’information. Sans alternatives publiques fortes, notre capacité d’action restera limitée.

En ce sens, nous plaidons pour une véritable politique d’infrastructure numérique publique, marquée par la neutralité du réseau, des réseaux sociaux décentralisés, un audit public des algorithmes et des modèles de rémunération qui valorisent les créateurs plutôt que l’exploitation des données. La relation avec la société civile doit également évoluer, car elle demeure encore trop descendante. Nous appelons à un partenariat plus protecteur et plus ouvert, incluant le soutien aux communautés OSINT, aux lanceurs d’alerte bien identifiés et aux hackers éthiques.

Et enfin, la montée en compétences est essentielle par la formation au sein de l’ensemble des services publics, mais aussi des entreprises et des collectivités locales, pour garantir une régulation réellement souveraine. Comment comptez-vous transformer structurellement notre écosystème ?

M. Nicolas Roche. Je ne sais guère comment répondre à ce qui relève davantage d’une affirmation que d’une question, voire d’une pétition de principe.

S’agissant de l’Arcom, vous avez entièrement raison ; il s’agit d’un acteur essentiel avec lequel nous entretenons des collaborations extrêmement étroites et permanentes. D’ailleurs, l’Arcom a publié très récemment, hier ou ce matin même, un rapport particulièrement intéressant, approfondi et très convergent avec la stratégie de lutte contre les manipulations de l’information que nous avons élaborée. Ce n’est évidemment pas un hasard. Nous avons besoin d’un régulateur national pleinement engagé, y compris dans la mise en œuvre du DSA, un régulateur actif et offensif dans ce domaine. Je ne peux, pour ma part, que me féliciter de la coopération extrêmement fructueuse qui existe aujourd’hui entre Viginum, le SGDSN et l’Arcom.

À ce titre, dans le modèle que nous avons construit progressivement pour la protection des élections, nous avons fait le choix, qui n’était pas totalement intuitif, de réunir autour de la table non seulement des administrations de l’État, le SGDSN, Viginum, le secrétariat général du gouvernement, le ministère de l’intérieur, mais également des autorités administratives indépendantes, au premier rang desquelles l’Arcom et la Commission du contrôle du financement de la vie politique. Ces autorités ont pleinement participé au réseau de coordination et de protection des élections, dans le respect intégral de leurs mandats, de leurs responsabilités et de leurs compétences spécifiques. Nous sommes un État de droit, mais cette collégialité témoigne du niveau de confiance qui existe aujourd’hui entre les régulateurs indépendants, chargés de missions de contrôle et de régulation, et les administrations de l’État. Plus l’Arcom figurera au cœur de notre dispositif, mieux nous nous porterons collectivement.

Sur la remise en cause du modèle économique des plateformes, qui relève davantage d’une ambition que d’une question, je dois dire, très honnêtement, que cette

ambition dépasse quelque peu les compétences qui sont celles du SGDSN. L'essentiel de ces très grandes plateformes sont aujourd'hui américaines et reposent sur un modèle économique fondé sur l'économie de l'attention. J'avoue rencontrer des difficultés à percevoir concrètement comment la puissance publique pourrait créer, à court ou moyen terme, des plateformes équivalentes. Si des idées existent, nous sommes évidemment preneurs, mais je ne sais pas, pour ma part, comment cela pourrait fonctionner.

Enfin, je souhaite revenir avec insistance sur ce que certains qualifient d'angle mort et qui, à nos yeux, n'en est absolument pas un. Je réaffirme avec force que le choix d'avoir placé la résilience, l'inclusion de la société civile et la diffusion large d'une responsabilité collective au cœur du premier pilier de la stratégie nationale de lutte contre les manipulations de l'information n'a rien d'un hasard. C'est un service de l'État régalien, le SGDSN à travers Viginum, qui a opéré le choix, inédit pour un service régalien, d'organiser des consultations extrêmement larges avec l'ensemble de la société civile, les experts et nos concitoyens, notamment à travers une consultation en ligne conduite avec Make.org.

C'est nous qui avons mis autour de la table le ministère de l'éducation nationale, le ministère de l'enseignement supérieur, les experts, les médias et l'ensemble des citoyens qui souhaitaient contribuer. Si nous avons placé la résilience, l'Académie de lutte contre les manipulations de l'information, l'éducation et la pédagogie au premier rang de la stratégie, c'est parce que nous savons très précisément ce que l'État central peut faire, mais aussi ce qu'il ne peut pas faire seul. Nous sommes convaincus que la défense de notre souveraineté démocratique et électorale exige une responsabilité distribuée et une mobilisation de l'ensemble de la nation. Cette conviction profonde irrigue la stratégie et guidera pleinement sa mise en œuvre.

M. Erwan Balanant (Dem). Avec la manipulation en croissante de l'information, la prolifération des phénomènes de désinformation et la précarisation du secteur des médias et de la presse, notre modèle informationnel est affaibli. Cet affaiblissement fait vaciller notre modèle démocratique et même civilisationnel. Pour ces raisons, je suis convaincu que notre modèle informationnel et culturel ne peut plus être considéré comme un « gentil » *soft power*.

Il doit devenir une pierre angulaire de la défense de notre démocratie, un instrument de coercition face aux ingérences étrangères pour préserver les valeurs portées par la France. Il n'est donc plus ni moins qu'un *hard power* en construction, qui doit devenir un pilier de notre souveraineté.

À la veille des élections présidentielles, nous ne pouvons pas nous passer d'outils de lutte. Vos conclusions vont dans le sens des États généraux de l'information, en rappelant que la régulation des plateformes et la protection d'un espace informationnel fiable, accessible et sécurisé, constituent des composantes nécessaires pour préserver notre souveraineté nationale. C'est dans cet esprit que le groupe Les Démocrates a inscrit à l'ordre du jour ma proposition de loi visant à renforcer l'effectivité des droits voisins, car une bonne presse est une presse en bonne santé financière, et représente un outil de lutte contre les désinformations. Cependant, votre stratégie souligne l'importance de la responsabilisation des plateformes et, comme vous l'avez rappelé, le rôle essentiel du droit pour lutter contre ces ingérences.

Comme vous le savez, les éditeurs de presse et des agences de presse sont pénalement responsables des contenus publiés. Devons-nous faire évoluer notre droit pour inventer une responsabilité éditoriale des plateformes ? Ainsi, au regard du droit européen, quels mécanismes opérationnels, *a minima* de coopération avec les grandes plateformes numériques, peuvent-ils être envisagés en France pour garantir une réponse réellement efficace ?

M. Nicolas Roche. Vous avez pointé du doigt une question essentielle, qui dépasse très largement mes compétences. C'est également une question qui relève des compétences de la commission de la culture et qui rejaillit sur l'ensemble des positions que le gouvernement, le premier ministre, la ministre de la culture et, évidemment, la ministre du numérique sont susceptibles de porter. Je ne préjugerai donc pas de leurs réponses respectives.

Le choix réalisé historiquement repose sur un constat factuel, un choix qui figure au fondement de la régulation européenne, lequel consiste à ne pas appliquer aux grandes plateformes cette obligation de responsabilité éditoriale.

Je considère pour ma part que, quelle que soit la réponse qui sera apportée par nos autorités politiques à cette question fondamentale touchant à notre modèle de droit de l'information, et qui me dépasse très largement, cette réponse prendra du temps. En revanche, je ne voudrais pas que cet élément nous empêche d'agir à court terme. En résumé, le débat que vous soulevez me dépasse très largement, mais il ne doit pas constituer un facteur d'inaction.

Ainsi, quelle que soit l'issue de ce débat, nous continuerons, à droit constant et notamment à droit européen constant, à utiliser pleinement l'ensemble des outils juridiques que nous avons collectivement mis du temps à élaborer, et pour lesquels la France s'est fortement engagée, y compris lorsqu'elle exerçait la présidence de l'Union européenne. Ce droit existe, nous devons le mettre en œuvre, et nous disposons d'instruments juridiques, tant nationaux qu'européens, dont il dépend de nous de faire un usage plein et entier.

Par ailleurs, en tant qu'administration de l'État, nous continuerons d'essayer d'objectiver divers sujets, en particulier la question des manipulations algorithmiques. Il s'agit d'un sujet complexe, dans la mesure où les algorithmes constituent de véritables « boîtes noires » ; ni les régulateurs ni les services de l'État n'y ont accès directement. Nous disposons bien souvent d'un accès très limité aux API, ce qui crée des contraintes techniques importantes. Malgré ces limites, nous travaillons, à droit constant, à développer des méthodes d'analyse qui nous permettront de nous forger une appréciation propre, fondée sur des critères techniques, scientifiques, réplicables et auditables. Cet axe de travail majeur nous occupera dans les mois à venir, en 2026. Il s'inscrit pleinement dans l'action des administrations de l'État.

M. Michel Criaud (HOR). Mon groupe Horizon et indépendant vous remercie pour la qualité de vos actions. Dans un contexte de multiplication des opérations d'ingérence numérique étrangère, et afin de lutter contre ces manipulations de l'information, la France a fait le choix de se doter d'une stratégie nationale structurée autour de quatre piliers.

Il s'agit tout d'abord, renforcer la résilience de la nation, de réguler les plateformes en ligne et les services offerts par l'intelligence artificielle générative. Il importe

également de consolider ses capacités opérationnelles de lutte contre les ingérences numériques étrangères, et de collaborer avec nos alliés européens et internationaux.

Je souhaite revenir sur ce deuxième pilier, pour souligner le recours croissant à l'intelligence artificielle (IA) dans le cadre d'opérations d'ingérence. En effet, un rapport d'information de mes collègues Alain David et Laetitia Saint-Paul, paru fin 2025, alerte sur l'éruption de l'intelligence artificielle dans les ingérences étrangères. La France serait ainsi l'une des cibles privilégiées des tentatives d'ingérences étrangères assistées par l'IA. Cette menace se matérialise aujourd'hui par des opérations d'influence numérique, de manipulation de l'information, et plus généralement par des stratégies de déstabilisation globale qui visent à saper la confiance dans les institutions, fragmenter l'opinion publique, et influencer les processus électoraux.

Dans ce contexte, comment appréhendez-vous concrètement le rôle de l'IA dans la lutte contre les manipulations de l'information, afin de protéger le débat public et défendre un espace informationnel fondé sur la liberté d'expression et la pluralité des opinions ?

M. Nicolas Roche. S'agissant de la question de l'intelligence artificielle, il faut rappeler que cette thématique fait pleinement partie de nos missions centrales. Je pense en particulier à l'évaluation de l'impact de l'IA sur un ensemble de sujets relevant de la sécurité nationale. À l'occasion du sommet sur l'intelligence artificielle de 2025, le président de la République a ainsi décidé la création de l'Institut national pour l'évaluation et de la sécurité de l'intelligence artificielle. Cette institution est d'ailleurs copilotée et codirigée par le SGDSN et par le directeur général des entreprises. Nous avons d'ailleurs tenu hier le troisième comité stratégique de l'Inesia, qui s'est doté d'une feuille de route rendue publique, dans une volonté assumée de transparence.

Cette feuille de route est accessible, y compris sur le site du SGDSN, et elle précise notamment le travail d'évaluation de l'Inesia sur les grandes questions d'impact de l'intelligence artificielle sur la sécurité nationale. À ce titre, nous visons principalement trois domaines : la prolifération nucléaire, radiologique, biologique et chimique (NRBC), la menace cyber et les manipulations de l'information et les INE. Ces axes de travail sont aujourd'hui pleinement engagés, à la fois au sein de Viginum et dans l'ensemble de l'écosystème de recherche français ou de différents *clusters* de recherche sur l'intelligence artificielle que nous avons réunis autour de la table. Nous avons construit un programme de recherche permettant une évaluation scientifique de l'impact de l'IA.

À ce stade, trois constats principaux se dégagent. Le premier concerne ce qui est le plus visible pour nos concitoyens dans l'utilisation de l'intelligence artificielle à des fins de manipulation de l'information, le *deepfake*. Il s'agit de la création de contenus synthétiques par des outils d'intelligence artificielle générative, qui imitent la réalité de manière de plus en plus convaincante et qui peuvent induire en erreur les utilisateurs des plateformes.

Pour autant, il ne s'agit pas de l'élément central de notre préoccupation. D'une part, nous parvenons à développer des outils de détection permettant de qualifier ces contenus synthétiques. D'autre part, l'enjeu majeur de la labellisation des contenus synthétiques se situe à l'interface entre la technologie et le droit. Il serait en effet préférable que ces contenus soient identifiés comme tels dès leur apparition sur les plateformes, plutôt que d'être détectés

a posteriori. Si cette question constituait notre seule difficulté en matière d'intelligence artificielle et de manipulation de l'information, la situation serait relativement satisfaisante.

En revanche, deux autres sujets sont beaucoup plus complexes et plus préoccupants. Il s'agit d'abord de l'utilisation de l'IA à des fins de massification et de réplication automatique des contenus. Je rappelle que la définition d'une ingérence numérique étrangère repose sur l'amplification inauthentique, délibérée et massive d'un contenu. Les plateformes disposent aujourd'hui de systèmes capables de détecter la réplication exacte d'un même texte ou d'une même image. Or, les outils d'intelligence artificielle permettent de répliquer ces contenus en y apportant des modifications marginales, ce qui permet de contourner les outils techniques de modération ou de détection des plateformes.

Ces techniques sont utilisées par nos adversaires pour diffuser de manière massive et automatique des contenus qui sont en réalité identiques dans leur intention, traduits dans différentes langues ou modifiés à la marge, afin de garantir un objectif central des opérations d'ingérence numérique étrangère, à savoir la masse et la visibilité. L'utilisation de l'intelligence artificielle dans ces manœuvres d'amplification massive inauthentique est aujourd'hui documentée et constitue un défi bien réel, d'autant plus que ces techniques gagnent en sophistication à mesure que les outils d'IA progressent. Nous savons les détecter et nous continuerons à le faire, mais l'effet de masse demeure un enjeu majeur.

Le dernier sujet, sur lequel je souhaite insister, n'est à ce stade pas documenté, mais il constitue un axe de recherche essentiel. Il s'agit de la pollution de modèles d'intelligence artificielle à des fins de manipulation de l'information, notamment par le *data poisoning*. Dans la construction d'un modèle d'intelligence artificielle, il existe une phase d'entraînement, puis une phase d'inférence. Pour un adversaire, l'objectif consisterait à faire en sorte que, lors de la phase d'inférence, le modèle fournisse naturellement des réponses orientées dans un sens déterminé, participant ainsi à une opération de manipulation de l'information.

Cela suppose d'examiner de manière structurelle la construction même des modèles d'IA afin d'identifier d'éventuelles opérations d'ingérence numérique étrangère. Il s'agirait alors de l'insertion de biais cognitifs ou de biais de réponse au sein des modèles, ce qui se rapproche, sans s'y confondre totalement, des questions de biais algorithmiques. À ce stade, nous n'avons pas documenté de modifications internes de modèles d'intelligence artificielle utilisées à des fins d'ingérence numérique étrangère. Toutefois, ce sujet figure au cœur de nos travaux de recherche, car si nous considérons cette hypothèse comme possible, il est raisonnable de penser que nos adversaires la considèrent également comme telle.

Ainsi, lorsque nous abordons la question de l'intelligence artificielle et des manipulations de l'information, nous examinons l'ensemble du spectre, depuis les *deepfakes* les plus simples jusqu'aux scénarios les plus complexes de pollution de modèles d'intelligence artificielle à des fins de manipulation de l'information.

M. le président Jean-Michel Jacques. Je cède à présent la parole aux députés intervenant à titre individuel.

Mme Delphine Batho (EcoS). Monsieur le secrétaire général, pouvez-vous établir un point d'étape concernant l'état de la menace en matière de désinformation

climatique ou scientifique en matière d'ingérence étrangère dans la période récente, notamment depuis le retrait des États-Unis de l'accord de Paris ?

Ensuite, il a naturellement été question des plateformes, mais le cadre juridique actuel ne doit-il pas être modifié pour tenir compte des relais intérieurs d'ingérence étrangère ? Enfin, même si cela dépasse le cadre de vos missions, je souligne que l'on ne peut se contenter d'une stratégie de défense sans disposer de volets contre-offensifs ou offensifs. En outre, les manipulations de l'information s'inscrivent dans un contexte d'ensemble. Pouvez-vous nous faire part de votre point de vue personnel sur ces sujets ?

Mme Sabine Thillaye (Dem). Monsieur le Secrétaire général, pouvez-vous préciser le contenu des travaux de l'Académie de lutte contre les manipulations de l'information ? Comment, en tant que simples citoyens, pouvons-nous développer un esprit suffisamment critique pour déterminer si l'on fait face ou non à une information d'ingérence étrangère, à partir de quelques éléments véritablement opérationnels et concrets ?

M. Romain Tonussi (RN). La révolution numérique a profondément transformé notre rapport à l'information. Si elle a permis de diversifier les sources et de limiter en partie la domination d'acteurs oligopolistiques, elle a aussi, dans le même temps, démultiplié les capacités de manipulation de l'information. Nous devons donc prendre la mesure de cette menace sans nous contenter de la penser comme un tout uniforme, car la désinformation ne cible pas indirectement les Français.

Deux publics me paraissent particulièrement vulnérables. Je pense d'abord aux populations ultramarines, qui, comme le souligne le rapport, sont souvent plus exposées aux ingérences en raison de leur situation géographique et informationnelle. Je pense ensuite aux jeunes, qui évoluent dans des environnements numériques massifs sans toujours disposer des outils critiques suffisants.

À cela s'ajoute un phénomène plus large : la fragmentation croissante des sociétés occidentales, qui isole les individus et crée un terrain favorable à la diffusion des récits de désinformation. Dans ce contexte, comment l'État peut-il bâtir une réponse différenciée, véritablement adaptée à ces publics et à ces vulnérabilités spécifiques ?

M. Nicolas Roche. Je n'ai pas beaucoup de doutes sur le fait qu'il existe aujourd'hui une quantité importante de désinformation scientifique et climatique, mais cela ne relève pas de mon mandat. En revanche, nous n'avons pas détecté ce phénomène au titre des ingérences numériques étrangères. La raison en est d'ailleurs assez simple : lorsque l'on observe la manière dont nos adversaires conduisent des opérations d'ingérences numériques étrangères, nous constatons que dans la quasi-totalité des cas, ils cherchent avant tout à produire du chaos et de la confusion, indépendamment du contenu lui-même. Tout est bon pour créer de la confusion, il n'existe pas de ciblage spécifique du thème scientifique et climatique dans ces opérations d'INE.

C'est précisément pour cette raison que je tiens à faire une distinction très claire entre les opérations d'INE en tant que telles et la question plus générale de la manière dont des acteurs, de façon ouverte, sans recourir à des campagnes inauthentiques et délibérées reposant sur des moyens numériques artificiels, produisent et diffusent des discours. Dans le monde ouvert, il est évident que la propagande anti-scientifique et anti-climatique existe, vous

le savez d'ailleurs mieux que moi. Toutefois, ce sujet n'est pas central pour nous lorsqu'il s'agit de la détection des opérations d'ingérences numériques étrangères.

Le deuxième point porte sur une question sur laquelle nous nous sommes longuement interrogés, notamment au moment de la construction de notre dispositif de protection des élections municipales, le réseau de coordination et de protection des élections (RCPE) : celle des relais intérieurs des ingérences étrangères. Ma réponse n'a pas vocation à me défausser de cette question, mais je tiens à rappeler qu'il ne s'agit pas de notre métier. Je ne nie absolument pas l'importance du sujet, mais je suis profondément convaincu que le niveau d'acceptabilité, par nos compatriotes et par nos concitoyens, et par vous-mêmes, de ce que l'État entreprend, suppose que l'on établisse une distinction extrêmement claire entre ce qui relève de l'étranger et ce qui relève du national, mais aussi entre ce qui relève de la technique et ce qui relève du contenu.

Je réinsiste donc sur le choix fondamental que nous avons fait : le dispositif que nous avons mis en place s'occupe de technologies et d'acteurs étrangers. Si, par la suite, des réflexions doivent être menées sur la question des relais intérieurs ou des acteurs nationaux, il s'agit d'un autre débat, qui me dépasse très largement et qui relève de la justice, du ministère de l'intérieur, de l'Arcom et des services de renseignement intérieur.

Je le redis avec force devant la représentation nationale : si nous avons été capables de mettre collectivement en place un dispositif que je considère aujourd'hui comme efficace, c'est parce que nous nous sommes tenus à une rigueur intellectuelle et sémantique constante, consistant à nous centrer sur les questions technologiques et sur les acteurs étrangers. La délégation parlementaire au renseignement peut d'ailleurs pleinement jouer son rôle dans ce cadre.

S'agissant de votre troisième question, je partage entièrement votre point de vue sur la nécessité de penser conjointement les dimensions défensives et offensives. Toutefois, offensif ne signifie pas symétrique. J'ai été l'un des partisans les plus engagés de la convergence entre nos dispositifs défensifs de détection et d'entrave des opérations d'ingérence numérique étrangère et le renforcement de notre stratégie de communication stratégique et de réponse. C'est précisément ce que nous faisons dans le cadre des efforts conjoints interministériels, qui associent en premier lieu le Quai d'Orsay et le SGDSN.

Dans la construction de notre dispositif interministériel, le ministère de l'Europe et des affaires étrangères assume la charge, la responsabilité et les compétences de fond, y compris linguistiques, pour porter notre message offensif de communication stratégique. Cela suppose que les moyens que nous utilisons soient des moyens légitimes. Pour le dire autrement, Viginum ne détecte pas et ne doit pas détecter des opérations qui ne seraient pas conformes à nos valeurs et à nos principes républicains. Dit autrement, répondre de manière offensive à la menace informationnelle ne signifie en aucun cas que nous devions adopter les techniques antidémocratiques et antirépublicaines de nos adversaires.

Je tiens donc à vous redire et à vous garantir que, de notre côté, nous sommes pleinement convaincus de la nécessité d'articuler intelligemment la dimension défensive et la dimension offensive de notre stratégie de réponse à la menace informationnelle, tout en demeurant strictement fidèles à nos principes et à nos valeurs démocratiques et républicaines.

S’agissant de l’Académie de lutte contre la manipulation de l’information, je constate avec e satisfaction l’intérêt considérable que ce projet suscite, et je veux y voir un encouragement pour l’ensemble des équipes. Nous sommes actuellement dans une phase de préfiguration, et sa mise en œuvre interviendra dans les semaines à venir. D’ores et déjà, un certain nombre d’actions ont été menées avant même leur labellisation sous l’intitulé d’Académie. Viginum a ainsi été très actif dans la construction de modules courts avec plusieurs médias, afin de transmettre notre connaissance technique et notre expertise à des journalistes qui exercent leur métier en toute indépendance, mais avec des compétences et des outils que nous leur avons transférés. Cela peut prendre la forme de travaux conjoints avec Arte ou d’autres partenaires pour produire des modules d’information et d’éducation à la lutte contre les manipulations de l’information.

Nous avons également travaillé avec le Centre de liaison de l’enseignement et des médias d’information (Clemi) dans le domaine pédagogique, pour élaborer des modules à destination des lycéens et des collégiens, afin de doter le monde éducatif d’outils permettant à d’autres acteurs de mener ce travail d’information, de sensibilisation et de pédagogie. C’est clairement dans cette direction que nous souhaitons poursuivre.

Votre remarque sur l’esprit critique va bien au-delà de ma fonction, mais elle fait profondément écho à ma conviction, en tant que chartiste, concernant le retour au texte et la critique des sources. Il s’agit là d’une exigence permanente pour chacun d’entre nous, mais qui nous conduit toutefois vers des champs qui relèvent davantage du ministère de l’éducation nationale, de l’enseignement supérieur et de la culture. Nous savons néanmoins, du côté des services régaliens de l’État, qu’il existe de nombreuses actions relevant de notre domaine de compétence et de notre périmètre de responsabilité, même si notre succès dépend aussi de facteurs qui ne dépendent pas de nous seuls, mais de l’engagement collectif des citoyens.

C’est précisément l’objectif du premier pilier de la stratégie de lutte contre les manipulations de l’information, qui concerne la résilience, lequel consiste à sortir du seul cadre régalien, pour aller au-delà. Nous partageons la conviction que, comme dans le domaine de la sécurité nationale, notre principal enjeu consiste à faire en sorte que ces sujets, pourtant très techniques, ne demeurent pas confinés au cercle restreint de la défense et de la sécurité nationale. Telle est la condition essentielle de notre succès. La même logique prévaut pour la LMI : il est indispensable que d’autres que les seuls spécialistes s’en saisissent.

Monsieur Tonussi, l’expérience montre effectivement que les outre-mer sont particulièrement exposés à la menace informationnelle. Nous avons documenté et publié des opérations, ou du moins des modes opératoires informationnels, attribuables, y compris en sources ouvertes, à un pays, l’Azerbaïdjan, qui a ciblé plusieurs territoires ultramarins, notamment la Nouvelle-Calédonie, avant d’essaimer ailleurs.

Nous sommes donc convaincus que les outre-mer sont surexposés à la menace informationnelle et qu’il est nécessaire de les aider à l’affronter. Nous avons engagé plusieurs actions, dont certaines relèvent de l’administration et ne sont pas publiques par nature. Je peux néanmoins indiquer que nous avons par exemple élaboré un guide spécifique à destination des préfets et des hauts-commissaires dans les outre-mer, afin de leur fournir, au niveau local, les instruments nécessaires pour travailler avec les partenaires territoriaux et élever le niveau de sensibilisation à la menace informationnelle.

Enfin, la question de la segmentation des publics et de leur exposition à la menace fait l'objet de nombreuses réflexions. À titre personnel, je suis de moins en moins convaincu que les jeunes constituent une cible prioritaire ou particulièrement vulnérable. Tout dépend de ce que l'on entend par « jeunes ». Les plus jeunes sont souvent, dans bien des cas, plus sensibilisés et informés que nous. Il n'existe donc pas d'équation simple entre âge et vulnérabilité particulière. En revanche, nous cherchons à adapter notre expertise technique aux différents publics, en tenant compte de l'âge, mais sans projeter des schémas de vulnérabilité préconçus. Notre défi consiste à transmettre un haut niveau de compétence technique à des publics aux profils très variés, en adaptant notre stratégie de résilience et de sensibilisation de manière différenciée et réaliste.

M. le président Jean-Michel Jacques. Je vous remercie pour vos propos captivants. J'apprécie en particulier votre approche participative et inclusive.

***

Information relative à la commission

La commission ***autorise*** *la publication sous forme de rapport d'information du recueil d'auditions du cycle sur la condition militaire, augmentées des contributions des groupes.*

***

La séance est levée à dix heures quarante-huit.

*

* *

Membres présents ou excusés

Présents. - Mme Delphine Batho, Mme Valérie Bazin-Malgras, M. Édouard Bénard, M. Christophe Bex, M. Hubert Brigand, M. Yannick Chenevard, Mme Caroline Colombier, M. Michel Criaud, M. José Gonzalez, Mme Florence Goulet, M. Daniel Grenon, M. David Habib, Mme Catherine Hervieu, M. Laurent Jacobelli, M. Jean-Michel Jacques, M. Pascal Jenft, M. Loïc Kervran, M. Abdelkader Lahmar, Mme Nadine Lechon, M. Didier Lemaire, Mme Michèle Martinez, M. Thibaut Monnier, Mme Josy Poueyto, Mme Natalia Pouzyreff, Mme Marie Récalde, M. Alexandre Sabatou, M. Aurélien Saintoul, M. Sébastien Saint-Pasteur, M. Thierry Sother, M. Thierry Tesson, Mme Sabine Thillaye, M. Romain Tonussi, M. Nicolas Tryzna

Excusés. - M. Christophe Blanchet, Mme Anne-Laure Blin, M. Matthieu Bloch, M. Frédéric Boccaletti, M. Manuel Bompard, M. Bernard Chaix, Mme Cyrielle Chatelain, Mme Geneviève Darrieussecq, M. Yannick Favennec-Bécot, M. Moerani Frébault, M. Guillaume Garot, M. Damien Girard, Mme Alexandra Martin, M. Aurélien Pradié, Mme Mereana Reid Arbelot, Mme Catherine Rimbert, Mme Marie-Pierre Rixain, M. Aurélien Rousseau, Mme Isabelle Santiago, M. Mikaele Seo, M. Boris Vallaud

Assistaient également à la réunion. - M. Erwan Balanant, M. Arnaud Saint-Martin