



# ASSEMBLÉE NATIONALE

17ème législature

## Ingérences étrangères en Nouvelle Calédonie

Question écrite n° 494

### Texte de la question

Mme Maud Petit attire l'attention de M. le ministre auprès du Premier ministre, chargé des outre-mer, sur la Nouvelle-Calédonie, collectivité d'outre-mer à statut particulier, bénéficie aujourd'hui d'un partage de souveraineté et d'une autonomie partielle et est plongée actuellement dans une grande instabilité, institutionnelle et démocratique. Dans ce contexte de crise et d'émeutes, il apparaît que des États étrangers cherchent à influencer les décisions politiques et institutionnelles locales à des fins stratégiques, géopolitiques et économiques. C'est ainsi que, le 18 avril 2024, l'assemblée nationale azérie a signé un mémorandum de coopération avec le Congrès de Nouvelle-Calédonie. Le 22 mai 2024, l'archipel a subi une cyberattaque d'une force inédite ; plusieurs IP russes auraient été découvertes, en lien avec cette attaque. Ces ingérences menacent la souveraineté française sur le sol de Nouvelle-Calédonie et dans la zone Pacifique et ébranlent aussi la stabilité politique et sociale de l'ensemble des régions et collectivités ultramarines. En juillet 2023, « l'initiative de Bakou » avait réuni, sous l'égide du Gouvernement azerbaïdjanais, les indépendantistes de Guyane, de Martinique, de Polynésie française et de Nouvelle-Calédonie. Hasard du calendrier, le Sénat a examiné récemment la proposition de loi visant à renforcer l'arsenal des mesures contre les ingérences étrangères que l'Assemblée nationale avait largement adoptée. Avec le contexte néocalédonien actuel, la proposition de loi a été élargie aux territoires d'outre-mer. Mme la députée souhaite connaître les mesures que M. le ministre entend mettre en œuvre contre ces ingérences étrangères, pour protéger la Nouvelle-Calédonie et, au-delà, l'ensemble des DROM-COM, qui représentent un atout géopolitique pour la France sur l'ensemble du globe. Mme la députée aimerait savoir quelles actions diplomatiques, numériques, économiques et pénales sont envisagées pour lutter contre ces tentatives de déstabilisation. Enfin, elle souhaite savoir comment le Gouvernement prévoit de sensibiliser ou d'impliquer les élus et populations locales dans cette lutte contre l'ingérence étrangère, afin de leur garantir le soutien de l'État qui veille à leur sécurité et à l'intégrité territoriale.

### Texte de la réponse

L'entité principale qui a en charge la lutte contre les ingérences étrangères (cyberattaques, tentatives de déstabilisation, etc.) est la direction générale de la sécurité intérieure (DGSI), rattachée au ministère de l'Intérieur. Elle joue un rôle essentiel dans la lutte contre les ingérences menaçant la souveraineté française, sur le plan préventif comme répressif, ainsi que le précise l'article 2, alinéa 2 du décret du 30 avril 2014 relatif aux missions et à l'organisation de la DGSI. Dans le cadre d'une commission d'enquête relative aux ingérences étrangères diligentée par le Sénat, le directeur de la DGSI a rappelé que la lutte contre les ingérences étrangères n'a cessé de prendre de l'importance, en termes de besoins comme en termes de moyens, en raison du contexte international et parce que la France y est particulièrement exposée. Face aux actes d'ingérence, la DGSI joue un triple rôle : - elle détecte et documente les comportements en cours, et renseigne les autorités à leur sujet. Pour mener à bien cette mission, la DGSI suit des relais qui, au sein de la société française servent de points d'appui à des actions d'espionnage ou à des politiques d'influence (association, monde universitaire, cultes...) ; - elle sensibilise au risque auquel chacun est exposé dans l'exercice de ses fonctions (domaines économique, universitaire, politique). La DGSI sensibilise largement les groupes politiques

au début de la législature et ces derniers ont des contacts réguliers avec les parlementaires, à leur demande ou d'initiative ; - elle riposte et entrave toute tentative d'ingérence sur l'ensemble du territoire. Dans ce cadre, la DGSi accorde une attention toute particulière aux territoires d'outre-mer, dont, à l'instar de l'ensemble de la communauté du renseignement, elle a conscience qu'ils sont encore plus directement exposés à des ingérences étrangères, notamment dans le Pacifique sud. S'agissant plus spécifiquement des ingérences étrangères à travers les manipulations de l'information, un travail pluridisciplinaire est mené en interministériel pour répondre à ce danger. Composantes à part entière des menaces hybrides, les manipulations de l'information ont l'objectif commun de perturber la sincérité du débat public. Compte tenu de la numérisation de nos sociétés, de la part croissante de notre débat public sur les réseaux sociaux et de l'importance de la liberté d'expression pour la démocratie, les campagnes numériques de manipulation de l'information sont susceptibles de porter atteinte aux intérêts fondamentaux de la Nation. Un certain nombre d'Etats, d'offices commerciaux ou de groupes d'opinion étrangers ont fait des manipulations d'information des outils au service de leurs objectifs stratégiques et les utilisent, parfois même comme des armes, dans le cadre de stratégies dites hybrides. Elles peuvent être différenciées selon trois niveaux de sophistication : - les offensives diplomatiques qui consistent le plus souvent à dévaloriser le modèle républicain, économique, sociétal de la France ainsi que ses alliances internationales, et à l'opposer au modèle souvent idéalisé du pays qui pilote ces opérations ; - les opérations de manipulation informationnelle qui diffusent des informations falsifiées, déformées, associées à de vraies informations pour les rendre crédibles, ou encore sorties de leur contexte ou partielles ; - enfin, les opérations de déstabilisation orchestrées et réalisées par des services de renseignement étrangers. Véritables actions secrètes, afin de ne pas remonter aux commanditaires, elles peuvent notamment exploiter des données piratées lors de cyberattaques et déformées lors de leur divulgation massive (hack and leak). Là encore, les outre-mer sont particulièrement touchés par ces tentatives, en raison de leur environnement géographique, de leur rapport spécifique à l'Etat, de leur histoire, mais aussi de leurs infrastructures. La France a su réagir de façon relativement précoce face à cette nouvelle menace en créant, le 14 juillet 2021, le service de vigilance et de protection contre les ingérences numériques étrangères, Viginum. Depuis sa création, ce service a obtenu des résultats probants en matière de détection. En complémentarité de Viginum, l'ensemble des services de renseignements de l'Etat combinent leurs compétences afin de pouvoir identifier les opérations de déstabilisation clandestines, de déterminer leurs éventuels commanditaires étatiques et de détecter les relais susceptibles de renforcer la légitimité et la crédibilité des narratifs. Ces missions sont assurées en coopération étroite avec les différents partenaires institutionnels habilités à traiter ce type de menaces. Viginum porte une attention particulière aux outre-mer, comme en témoigne la publication le 2 décembre de son rapport "UN-notorious BIG : une campagne numérique de manipulation de l'information ciblant les DROM-COM et la Corse". En complémentarité avec l'action de Viginum, l'ANSSI (Agence nationale pour la sécurité des systèmes d'information) intervient dans l'ensemble des territoires ultramarins par le biais d'opérations de cyberdéfense et propose des parcours de cybersécurité aux acteurs locaux (collectivités, établissements publics...). Ces parcours d'accompagnement permettent à ces acteurs de réaliser des diagnostics de cybersécurité et de mettre en place des actions de sécurisation numérique (données, système d'information, protection du réseau). L'ANSSI a d'ailleurs financé des centres de ressource outre-mer avec l'inauguration entre octobre et décembre 2024, du Centre Cyber Pacifique (Nouvelle-Calédonie), de la marque Cyber Réunion et du CSIRT La Réunion 04/12/24 et l'inauguration du CSIRT Atlantic intégré au sein de l'Agence Caribéenne de Cybersécurité (ACCYB). Signe de la sensibilité ultramarine particulière de l'ANSSI, un délégué aux outre-mer a été nommé en 2022. L'ANSSI a également adhéré au réseau PaCSON en juin 2024 avec un statut de partenaire (après le FBI, la Cybersecurity and Infrastructure Security Agency (CISA), le Forum of Incident Response and Security Teams (FIRST) et la Reserve Bank of Fiji). En juillet 2024, le Canadian Centre for Cyber Security (CCCS) est devenu le cinquième partenaire de PaCSON. Le Royaume-Uni envisagerait également une adhésion via son NCSC-UK. PaCSON est un réseau regroupant 17 Etats membres ou partenaires situés en zone Pacifique Sud. Il a été créé en 2017 à l'initiative du gouvernement australien, dans le cadre de son programme régional de renforcement des capacités de cybersécurité et vise à promouvoir le partage d'informations et le renforcement des capacités de cybersécurité. De plus, l'ANSSI pilote la transposition de la directive dite "NIS2" (Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union), qui sera applicable à l'identique en Nouvelle-Calédonie. Sur le plan législatif, la loi relative à la manipulation de l'information du 20 novembre 2018 permet également d'imposer l'obligation de transparence et de coopération pour les plateformes qui doivent

notamment signaler les contenus sponsorisés, et crée une action judiciaire en référé pour faire cesser rapidement la circulation de fausses informations dès lors qu'elle est manifeste, diffusée massivement et de manière artificielle et a vocation de troubler la paix publique ou la sincérité d'un scrutin. De plus, la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France a été publiée au journal officiel du 26 juillet 2024. Ce texte vise à renforcer le dispositif de prévention et d'entrave aux ingérences ou tentatives d'ingérences étrangères qui se multiplient dans l'hexagone et au sein des territoires ultramarins. Les élus seront pleinement informés de l'état des menaces et des modalités d'exécution des dispositifs mis en place par l'Etat, car cette loi prévoit la remise par le Gouvernement au parlement, avant le 1er juillet 2025 puis tous les deux ans, d'un rapport sur l'état des menaces qui pèsent sur la sécurité nationale. Enfin, au-delà de ce travail interministériel et des « garde-fous » mis en place pour contrer les manipulations de l'information d'origine étrangère visant à porter atteinte aux intérêts fondamentaux de la nation, le sujet est traité par un large éventail d'acteurs de la société civile : - l'apport irremplaçable des médias de qualité qui consacrent une part importante de leurs moyens à la vérification des faits et à la révélation des impostures ; - le monde de la recherche qui a investi ce sujet avec beaucoup d'engouement. A ce titre, les filières universitaires de formation ont commencé à alimenter un vivier national de jeunes experts et les laboratoires de recherche mènent leurs travaux, indépendamment de ceux de l'administration, mais de façon tout à fait complémentaire.

### Données clés

**Auteur :** [Mme Maud Petit](#)

**Circonscription :** Val-de-Marne (4<sup>e</sup> circonscription) - Les Démocrates

**Type de question :** Question écrite

**Numéro de la question :** 494

**Rubrique :** Outre-mer

**Ministère interrogé :** [Outre-mer](#)

**Ministère attributaire :** [Outre-mer](#)

### Date(s) clé(s)

**Question publiée au JO le :** [8 octobre 2024](#), page 5212

**Réponse publiée au JO le :** [18 mars 2025](#), page 1854