PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Réseau de coordination et protection des élections

18 juin 2026 | n°01

Face à la menace d'ingérence numérique étrangère en période électorale, les pouvoirs publics français ont décidé de renforcer le dispositif national de protection des élections via la création du **réseau de coordination et de protection des élections (RCPE)**. Mis en place durant la période des élections municipales de mars 2026, le RCPE est chargé d'effectuer des **points de situation** sur la menace d'ingérences numériques étrangères pesant sur le scrutin, de proposer le cas échéant la **mise en œuvre de mesures de réponse**, et **d'informer le grand public de manière régulière et périodique.**

Dans le cadre des élections provinciales en Nouvelle-Calédonie du 28 juin 2026, le RCPE a été reconduit. Il est **composé d'administrations et d'autorités indépendantes compétentes en matière électorale** (l'Arcom, la CNCCFP, le secrétariat général du Gouvernement, le ministère de l'Intérieur, le Haut-Commissariat de la République en Nouvelle-Calédonie, VIGINUM et le Comité éthique et scientifique, chargé de suivre son activité), et est coordonné par le Secrétariat général de la défense et de la sécurité nationale (SGDSN).

Qu'est qu'une ingérence numérique étrangère ?

Composantes à part entière des menaces dites « hybrides », les ingérences numériques étrangères font peser une menace réelle et sérieuse sur la cohésion nationale et nos démocraties. Définie par le décret n°2021-922 du 13 juillet 2021, une opération d'ingérence numérique étrangère est constituée par la réunion de quatre critères : (i) l'implication d'un **État étranger ou une entité non-étatique étrangère** ; (ii) la diffusion **artificielle ou automatisée, massive et délibérée** ; (iii) des allégations ou imputations de faits manifestement inexactes ou trompeuses ; (iv) une volonté de porter atteinte aux **intérêts fondamentaux de la Nation**.

Prenant la forme de campagnes planifiées ou d'actions opportunistes, ces manœuvres utilisent des procédés techniques (faux comptes, faux sites *web*, détournement d'outils d'intelligence artificielle générative, etc.) pour amplifier, de manière inauthentique, la diffusion ou la visibilité de contenus en vue de poursuivre une finalité malveillante.

Le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM), rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), est le service technique et opérationnel chargé de détecter et de caractériser les opérations d'ingérence

numérique étrangères. Strictement encadrée par le décret n°2021-922 du 13 juillet 2021, complété par le décret n°2026-70 du 11 février 2026, l'activité opérationnelle de VIGINUM consiste en la conduite **d'investigations techniques menées en source ouverte**, impliquant la collecte et l'analyse de données **publiquement accessibles sur les plateformes en ligne,** afin de déceler la mise en œuvre de **procédés inauthentiques** par des **acteurs étrangers malveillants**.

Pourquoi les élections en Nouvelle-Calédonie sont-elles une cible ?

Fondements de la vie démocratique, les élections constituent une cible de choix pour des acteurs étrangers malveillants désireux de déstabiliser les institutions, le processus électoral en lui-même ainsi que la cohésion sociale. En France, comme dans d'autres pays, la menace d'ingérence numérique étrangère en période électorale est désormais concrète depuis plusieurs années.

En 2024, VIGINUM a ainsi détecté et caractérisé 25 tentatives d'ingérence numérique étrangères lors des élections européennes et législatives. Lors des élections municipales de mars 2026, quatre ingérences numériques étrangères ont été détectées et exposées par le RCPE. Elles sont décrites dans le rapport « Protection du débat public contre les ingérences numériques étrangères durant les élections municipales des 15 et 22 mars 2026 ».

En raison de son environnement stratégique et des spécificités de son histoire, la Nouvelle-Calédonie est un territoire ultra-marin susceptible de faire l'objet de manœuvres de déstabilisation. En effet, depuis 2023, la Nouvelle-Calédonie a déjà fait l'objet d'opérations d'ingérence numérique étrangère précédemment caractérisées par VIGINUM (cf infra). Organisées le 28 juin 2026, les élections provinciales sont donc susceptibles d'être ciblées par ce type d'opérations.

Point de situation sur la menace d'ingérence numérique étrangère ciblant la Nouvelle-Calédonie

Bien qu'**à ce stade**, **aucune tentative ou opération d'ingérence numérique étrangère ciblant spécifiquement les élections provinciales du 28 juin n'ait été caractérisée**, VIGINUM est en mesure de dresser un premier panorama de cette menace, émanant d'acteurs ayant déjà mené des opérations informationnelles ciblant la Nouvelle-Calédonie. À l'approche du scrutin, le service se montrera ainsi particulièrement vigilant quant aux menaces suivantes :

◊ Menace informationnelle émanant des acteurs pro-azerbaïdjanais

Depuis 2023, VIGINUM suit les activités numériques d'acteurs pro-azerbaïdjanais visant à porter atteinte aux intérêts français dans le champ informationnel. En mai 2024, VIGINUM avait ainsi publié une fiche technique relative à une opération d'ingérence numérique étrangère émanant de ces acteurs et s'inscrivant dans le contexte des émeutes en Nouvelle Calédonie.

VIGINUM a par ailleurs caractérisé l'activité malveillante de l'organisation azerbaïdjanaise du *Baku Initiative Group,* officine liée au pouvoir azerbaïdjanais menant des actions de de déstabilisation contre ses adversaires. Celle-ci a mené plusieurs opérations d'ingérence numérique étrangères visant à remettre en cause la souveraineté de la France dans ses territoires ultramarins, et notamment en Nouvelle-Calédonie, via l'instrumentalisation des mouvements et idées indépendantistes. En décembre 2024, VIGINUM avait ainsi publié un rapport technique sur le sujet.

Si l'activité numérique du BIG est moindre depuis l'été 2025, celui-ci a de nouveau ciblé la France, et plus particulièrement la Nouvelle-Calédonie, de manière opportuniste en mai 2026, par le biais de

plusieurs publications sur ses comptes *X*, *Facebook* et *Instagram,* notamment relatives au dégel du corps électoral en vue des élections provinciales. Bien qu'elles aient bénéficié d'une amplification artificielle et coordonnée, ces publications n'ont bénéficié que d'une faible visibilité sur les réseaux sociaux.

◊ Menace informationnelle émanant des acteurs pro-PCC

Le dispositif informationnel numérique pro-PCC ciblant les audiences en Indopacifique conteste principalement la présence, notamment militaire, des États-Unis et des autres États occidentaux, dont la France, dans la région.

VIGINUM a déjà pu observer par le passé l'instrumentalisation des sujets liés à la Nouvelle Calédonie par l'écosystème informationnel pro-PCC,à l'aide de moyens coordonnés et inauthentiques à destination d'une audience sinophone.