

Réseau de coordination et de protection des élections

30 janvier 2026 | n° 1

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 par la création du **réseau de coordination et de protection des élections (RCPE)**. Ce réseau 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, VIGINUM et le Comité éthique et scientifique, chargé de suivre son activité. Ce réseau est coordonné par le Secrétariat général de la défense et de la sécurité nationale (SGDSN). Le RCPE est chargé d'évaluer **la menace d'ingérences numériques étrangères** pendant la période des élections municipales, de proposer le cas échéant la **mise en œuvre de mesures de réponse, d'informer le grand public de manière régulière et périodique**.

Qu'est-ce qu'une ingérence numérique étrangère ?

Composantes à part entière des menaces dites hybrides, les ingérences numériques étrangères sont une menace réelle et sérieuse sur le processus électoral. Définie par le décret n° 2021-922 du 13 juillet 2021, une opération d'ingérence numérique étrangère est définie par quatre critères : l'implication d'un **État étranger ou une entité non-étatique étrangère** ; la diffusion **artificielle ou automatisée, massive et délibérée** ; des allégations ou imputations de faits manifestement inexacts ou trompeuses ; 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 comme les faux comptes, de faux sites *web*, le détournement d'outils d'intelligence artificielle générative pour amplifier, de manière inauthentique, la diffusion ou la visibilité de contenus.

Le [service de vigilance et de protection contre les ingérences numériques étrangères](#) (VIGINUM), composante du [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 étrangère. Strictement encadrée par le décret n° 2021-1587 du 7 décembre 2021, 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 sont-elles une cible ?

Fondements de la vie démocratique, les élections constituent une cible de choix pour des acteurs étrangers malveillants désireux d'en déstabiliser le bon déroulement. En France, comme dans d'autres pays, la menace d'ingérence numérique étrangère en période électorale est avérée depuis plusieurs années : en 2024, VIGINUM a détecté et caractérisé 25 tentatives d'ingérence numérique étrangères lors des élections européennes et législatives.

Pourquoi créer un réseau de coordination et de protection des élections pour les élections municipales de 2026 ?

Les 15 et 22 mars 2026, les électeurs seront appelés aux urnes lors des élections municipales. Cette élection est une cible pour des acteurs étrangers désireux de déstabiliser le débat public en ligne. En se fondant sur l'expérience de pays partenaires, un dispositif national renforcé de protection des élections face aux ingérences numériques étrangères a été mis en place. Il prend la forme d'un **réseau de coordination et de protection des élections (RCPE)**. Le RCPE **rassemble des administrations et des autorités indépendantes compétentes en matière électorale** : l'[Autorité de régulation de la communication audiovisuelle et numérique](#) (Arcom), la [Commission nationale des comptes de campagne et des financements politiques](#) (CNCCFP), le [secrétariat général du Gouvernement](#), le [ministère de l'intérieur](#), VIGINUM et le Comité éthique et scientifique, institué auprès du Secrétaire général de la défense et de la sécurité nationale, chargé de suivre l'activité du service VIGINUM. L'animation et la coordination de ce réseau sont assurées par le SGDSN.

Le RCPE a pour missions d'évaluer, **chaque semaine**, l'état de la menace d'ingérences numériques étrangères durant la période électorale, d'envisager **les mesures de réponse** adéquates face aux risques éventuels de déstabilisation du scrutin, et **d'informer les citoyens**, en **garantissant le respect des principes de transparence et d'intégrité du débat démocratique en période électorale**.

En cas d'**ingérence numérique étrangère susceptible d'altérer l'information des citoyens pendant la période électorale**, les membres du réseau apprécieront la situation et seront consultés par le SGDSN sur **l'opportunité d'activer un certain nombre de leviers de réponse** : la saisine de l'autorité judiciaire, l'information des équipes de campagnes, la mobilisation des institutions chargées du bon déroulement des élections, la dénonciation publique de l'ingérence. Par ailleurs, chaque organisme membre du RCPE demeure compétent pour mettre en œuvre les actions relevant de ses prérogatives juridiques.

Le RCPE s'est réuni pour la première fois le 21 janvier 2026. **À compter du 4 février 2026, le RCPE se réunira de manière hebdomadaire. Chaque réunion du RCPE fera l'objet d'un bulletin d'information public, accessible sur le site du SGDSN.**

Point de situation sur la menace d'ingérences numériques étrangères ciblant les élections municipales 2026

À ce stade, aucune tentative ou opération d'ingérence numérique étrangère ciblant spécifiquement les élections municipales 2026 n'a été caractérisée.

VIGINUM observe toutefois régulièrement quatre grandes stratégies malveillantes en période électorale, en France comme à l'étranger. Ces stratégies sont susceptibles d'être utilisées pendant la période électorale pour cibler les scrutins de mars 2026.

◇ **Décrédibiliser la procédure électorale**

Cette stratégie a pour objectif de délégitimer le processus électoral pour pouvoir en contester le résultat, notamment en le présentant comme faussé, insincère, inutile, voire manipulé par les autorités garantes de son bon fonctionnement.

Exemple : dans le cadre de l'élection présidentielle américaine de 2024, des élections fédérales allemandes et des élections législatives moldaves de 2025, [le mode opératoire informationnel russe Storm-1516](#) a été employé pour décrédibiliser les procédures électorales, en affirmant que les bulletins de votes avaient été trafiqués ou détruits pour nuire à certains candidats. Ce récit trompeur est susceptible d'être déployé *via* les procédés techniques des faux comptes ou de sites *web* créés pour l'occasion.

Semaine du 26 janvier : aucune opération d'INE servant cette stratégie n'a été détectée.

◇ **Alimenter la défiance vis-à-vis des médias du pays visé**

Cette stratégie vise à délégitimer les médias pour remettre en question l'authenticité des informations diffusées, semer la confusion et pousser les citoyens à se réorienter vers des sources d'informations inauthentiques, manipulées ou fabriquées de toutes pièces, administrées par des acteurs étrangers.

Exemple : depuis février 2025, des opérateurs liés au mode opératoire informationnel pro-russe *Storm-1516* ont lancé une campagne probablement destinée à se prépositionner dans l'espace informationnel francophone. Cette campagne prend la forme d'enregistrements de plus d'une centaine de noms de domaines en « .fr » imitant des sites de presse locaux, dont certains demeurent actifs et alimentés par des articles de presse générés par des outils d'intelligence artificielle.

Semaine du 26 janvier : une campagne malveillante en cours. À ce stade, cette campagne n'a qu'une très faible visibilité.

◇ **Exposer la réputation d'un(e) candidat(e) ou d'un parti politique**

Cette stratégie a pour objectif de modifier la perception d'un(e) candidat(e) auprès de l'opinion en le dénigrant ou en le promouvant, à travers différentes tactiques, techniques et procédures.

Exemple : les acteurs d'un dispositif informationnel chinois ont par le passé ciblé certains candidats s'étant ouvertement exprimés sur des problématiques d'importance pour la Chine, à l'instar de ce qui a été observé lors des élections européennes de 2024

Semaine du 26 janvier : aucune opération d'INE servant cette stratégie n'a été détectée.

◇ **Instrumentaliser certaines thématiques afin de polariser le débat public numérique**

Cette stratégie consiste pour une puissance étrangère à amplifier de manière artificielle ou inauthentique la visibilité de sujets considérés comme sensibles et/ou susceptibles d'influencer la décision des électeurs, afin de nourrir la polarisation du débat public et accroître les divisions de la société.

Exemple : dans le cadre de divers mouvements sociaux en France, plusieurs modes opératoires informationnels ont cherché à s'immiscer dans le débat public numérique afin d'amplifier la visibilité de ces sujets sur les réseaux sociaux, notamment par la récupération de *hashtags*. Leur visibilité demeure toutefois relativement faible.

Semaine du 26 janvier : aucune opération d'INE servant cette stratégie n'a été détectée.

Contacts presse

Gwenael.Jezequel@sgdsn.gouv.fr

Viginum_presse@sgdsn.gouv.fr