PREMIER
MINISTRE

Liberté
Égalité
Fraternité

Protection du débat public contre les ingérences numériques étrangères durant **les élections municipales des 15 et 22 mars 2026**

Rapport public

Juin 2026

Table des matières

Avant-propos : les élections, cibles privilégiées des ingérences numériques étrangères 2

1. Le réseau de coordination et de protection des élections 3

1.1 Principes directeurs du RCPE 3

1.2 Missions, organisation et fonctionnement du RCPE 3

1.3 Préparation préalable avec les acteurs du scrutin 5

1.3.1 Acteurs politiques 5

1.3.2 Médias et grand public 5

1.3.3 Plateformes 5

2. Panorama des INE observées durant les élections municipales 2026 7

2.1 Tendances de la menace 7

2.1.1 Quatre stratégies de déstabilisation du débat public national en période électorale 7

2.1.2 Entre persistance et évolution de la menace 7

2.2 Ingérences numériques étrangères observées durant les élections municipales de 2026 8

2.2.1 Deux INE conduites au moyen de MOI pro-russes persistants 8

2.2.2 Une INE à finalité lucrative conduite au moyen d'un nouveau MOI impliquant un acteur non-étatique localisé au Vietnam. 10

2.2.3 Une INE ciblant des candidats du parti *La France Insoumise* conduite au moyen d'un nouveau MOI impliquant un acteur non-étatique localisé en Israël 14

3. Synthèse de l'action du RCPE et mesures d'atténuation de la menace 20

3.1 Appréciation de la menace détectée et caractérisée 20

3.1.1 De la difficulté d'évaluer les effets d'une ingérence numérique étrangère sur le débat public numérique 20

3.1.2 Une visibilité limitée des INE détectées durant la campagne électorale 21

3.2 Réponses et mesures d'atténuation mises en œuvre 21

3.2.1 L'information des acteurs victimes d'opérations d'ingérence numérique étrangère 21

3.2.2 Une communication transparente et régulière 22

3.2.3 La coopération avec les fournisseurs de très grandes plateformes en ligne et moteurs de recherche 22

4. Bilan et grands enseignements pour 2027 24

4.1 Réactivité opérationnelle du dispositif 24

4.2 Intérêt de la coordination préalable avec les acteurs politiques et médiatiques 24

4.3 Vertu de la régularité et de la périodicité de la communication 25

4.4 Efficacité de l'atténuation des risques en lien avec les fournisseurs de plateformes en ligne 25

5. Lexique des ingérences numériques étrangères 27

Avant-propos : les élections, cibles privilégiées des ingérences numériques étrangères

Dans un contexte international marqué par une conflictualité numérique globale croissante, les opérations d'ingérence numérique étrangère sont devenues un instrument central des rapports de force contemporains. Conduites tant par des acteurs étatiques que non-étatiques étrangers, ces opérations visent notamment à porter atteinte au fonctionnement des processus démocratiques, à affaiblir les intérêts des parties ciblées, ou encore à promouvoir les priorités stratégiques de compétiteurs hostiles.

En tant que symbole et fondement de la vie démocratique, les élections constituent à ce titre une cible de choix pour des acteurs étrangers malveillants désireux d'en déstabiliser le bon déroulement. Depuis l'élection présidentielle de 2017 en France, aucun rendez-vous électoral ou référendaire majeur n'a en effet été épargné par des tentatives de manipulations de l'information impliquant des acteurs étrangers. Par ailleurs, le retour d'expérience des récents scrutins qui se sont tenus en Europe ces deux dernières années (Moldavie, Allemagne, Roumanie, Pologne, Hongrie, *etc.*) atteste d'un niveau préoccupant de menace.

Dernier processus électoral national au suffrage universel direct avant le scrutin présidentiel de 2027, les élections municipales des 15 et 22 mars 2026 étaient ainsi susceptibles de constituer une cible de premier plan pour les compétiteurs stratégiques de la France. Si les enjeux locaux peuvent parfois demeurer difficiles à appréhender pour des acteurs étrangers malveillants, plusieurs facteurs ont amené VIGINUM à considérer le niveau de menace d'ingérence numérique étrangère sur le scrutin comme élevé. En effet, le contexte international volatil et la forte pénétration des sujets européens et internationaux dans le débat politique français (guerre en Ukraine, traité UE-Mercosur, relation transatlantique, conflit au Moyen-Orient), combinés à un calendrier politique national spécifique, étaient susceptibles de constituer un terrain propice à la conduite d'opérations d'ingérence numérique étrangère lors de ce scrutin.

Dans ce contexte, et 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 pour les élections municipales des 15 et 22 mars 2026, avec la création du réseau de coordination et de protection des élections (RCPE).

1. Le réseau de coordination et de protection des élections

1.1 Principes directeurs du RCPE

Face au constat d'une menace croissante d'ingérence numérique étrangère (INE) pouvant peser sur les rendez-vous électoraux, un dispositif national renforcé de protection des élections face aux ingérences numériques étrangères a été mis en place, sous la forme d'un nouveau réseau de coordination et de protection des élections (RCPE). La création de ce réseau s'est appuyée sur un ensemble de principes directeurs, partiellement inspirés de l'expérience canadienne[1] :

- **l'impartialité** du suivi d'une menace impliquant des acteurs exclusivement étrangers, susceptibles de viser tous les candidats, l'objectif étant la préservation de la souveraineté de notre débat public numérique en contexte électoral ;
- **la neutralité** d'un réseau de coordination où ne siègent que des représentants de l'administration et d'autorités administratives indépendantes ;
- **l'objectivité** garantie par une analyse technique et technologique des modes opératoires informationnels inauthentiques impliquant des acteurs étrangers, sans appréciation des opinions, des acteurs ou des mouvements structurant le débat interne ;
- **la transparence** matérialisée par la publication, *a minima* une fois par semaine, d'un bulletin public d'information décrivant l'état des opérations d'ingérence numérique étrangère détectées et caractérisées ;
- **le fonctionnement précoce et routinier** du dispositif de protection, dès le début du mois de janvier 2026 et réuni au minimum chaque semaine, pour assurer sa réactivité et sa collégialité.

1.2 Missions, organisation et fonctionnement du RCPE

Mis en place à compter du 7 janvier 2026, **le RCPE** a vocation à éclairer collégialement la prise de décision du Secrétaire général à la défense et à la sécurité nationale, ainsi que celle de chacun de ses membres dans leurs champs de compétences respectifs.

Animé et coordonné par le Secrétariat général de la défense et de la sécurité nationale (**SGDSN)** en application de sa mission de protection contre les opérations d'INE[2], le RCPE rassemble des administrations et des autorités indépendantes compétentes en matière électorale :

- **l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom)**, autorité publique indépendante, en sa qualité de garante de la liberté de communication audiovisuelle en France, et désignée coordinateur national pour les services numériques ;
- **la Commission nationale des comptes de campagne et des financements politiques (CNCCFP)**, autorité administrative indépendante, au titre de sa mission de contrôle des dépenses de campagne électorale et des financements des partis politiques français ;
- **le Secrétariat général du Gouvernement (SGG)**, en vertu de son expertise juridique ;
- **le ministère de l'Intérieur**, chargé de l'organisation des élections politiques, avec le concours de la **Direction générale des outre-mer** pour ce qui relève de ses compétences ;
- **VIGINUM**, au titre des missions de détection et de caractérisation des ingérences numériques étrangères qui lui sont confiées par le décret n° 2021-922 du 13 juillet 2021[3] ;
- **le Comité éthique et scientifique**, institué auprès du Secrétaire général de la défense et de la sécurité nationale, chargé de suivre l'activité de VIGINUM.

---

[1] Dès 2019, le Canada a en effet instauré un protocole public en cas d'incident électoral majeur (PPIEM), actualisé à l'occasion des 45èmes élections générales de 2025.

[2] Voir l'article R.* 1132-3 du code de la défense.

[3] Révisé par le décret n° 2026-70 du 11 février 2026.

Le rôle de VIGINUM en période électorale

Le 13 juillet 2021, la France s'est dotée d'un 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). VIGINUM a notamment pour mission, en période électorale, de :

- « détecter, caractériser et documenter, en analysant les données accessibles publiquement sur les plateformes en ligne, sur les moteurs de recherche en ligne ainsi que sur les interfaces en ligne [...] lorsque celles-ci sont de nature à altérer l'information des citoyens pendant les périodes électorales » ;
- « assister le secrétaire général de la défense et de la sécurité nationale dans sa mission d'animation et de coordination des travaux interministériels en matière de protection contre les opérations d'ingérence numérique étrangère et d'anticipation des menaces qu'elles représentent » ;
- « fournir toute information utile [...] à l'Arcom [notamment] en vue de participer à la supervision de la mise en œuvre effective de l'obligation d'atténuer les risques systémiques [au sens du Règlement européen sur les services numériques] » et « à toute autorité, y compris juridictionnelle, saisie à l'occasion d'élections politiques ».

Pour ce faire, le service mène des investigations en source ouverte afin de documenter et caractériser techniquement les phénomènes inauthentiques présentant des marqueurs d'extranéité (comptes suspects, contenus malveillants, comportements anormaux ou coordonnés) qui se manifestent sur les plateformes et interfaces en ligne. Une ingérence numérique étrangère est définie par quatre critères :

- **son contenu :** les allégations ou imputations de faits manifestement inexacts ou trompeurs ;
- **son comportement :** l'usage de moyens inauthentiques de diffusion visant à amplifier artificiellement la visibilité d'un contenu (*bots*, trolls, avatars, *etc.*) ;
- **sa finalité :** l'atteinte aux intérêts fondamentaux de la Nation ;
- **ses auteurs** : l'implication directe ou indirecte d'un acteur étranger (étatique, paraétatique ou non-étatique). L'origine géographique des actifs numériques ou des intermédiaires techniques caractérisés peut différer de l'origine du commanditaire.

En période électorale, VIGINUM est ainsi compétent pour détecter et caractériser les campagnes numériques de manipulation de l'information impliquant des acteurs étrangers et de nature à altérer l'information des citoyens. Le Service fournit également toute information utile aux autorités garantes du bon déroulement du scrutin.

Chaque semaine entre le 21 janvier et le 25 mars 2026, le RCPE a ainsi évalué l'état de la menace d'ingérence numérique étrangère pesant sur le scrutin, débattu des mesures de réponse adéquates, et informé les citoyens, en garantissant le respect des principes de transparence et d'intégrité du débat démocratique en période électorale. En présence d'une menace d'INE détectée et caractérisée par VIGINUM, les leviers de réponse pouvant être mobilisés par le RCPE étaient les suivants :

- **l'information des acteurs ciblés,** en particulier des partis des candidats et des médias ciblés, ou le cas échéant du réseau préfectoral, afin de sécuriser l'organisation du scrutin ;
- **le partage d'informations techniques aux plateformes**, ou le cas échéant le signalement de contenu illicite dans le cadre du dispositif PHAROS du ministère de l'Intérieur ;
- **la publication ou la dénonciation publique** d'une tentative d'INE ou d'une INE ciblant la France ou ses intérêts fondamentaux ;

- **le signalement à l'autorité judiciaire** de tout fait susceptible de revêtir une qualification pénale en application de l'article 40 du code de procédure pénale ou, lorsqu'applicable, la saisine de l'autorité judiciaire en référé, dans le but d'obtenir des mesures conservatoires.

Les membres du RCPE demeurent compétents pour mettre en œuvre les actions relevant de leurs prérogatives, conformément à leurs cadres juridiques respectifs.

1.3 Préparation préalable avec les acteurs du scrutin

Afin de contribuer à renforcer la résilience nationale en amont du scrutin, des actions de sensibilisation sur la menace d'ingérence numérique étrangère en contexte électoral ont été menées les mois précédents par des membres du RCPE, à destination des acteurs politiques, des médias et des plateformes.

1.3.1 Acteurs politiques

Le SGDSN a rencontré au cours des mois de décembre 2025 et janvier 2026 :

- les présidents de l'Assemblée nationale et du Sénat ;
- les présidents des commissions chargées de la culture, de la défense et des lois de l'Assemblée nationale et du Sénat ;
- les représentants de l'association des Maires de France, de l'ARF (Association des régions de France), de *France Urbaine*, d'Interco, de l'association des communes et collectivités d'Outre-Mer ;
- la totalité des dirigeants des groupes politiques et partis représentés à l'Assemblée nationale et au Sénat.

Le SGDSN a également organisé une séance de sensibilisation le 28 janvier 2026 à destination de tous les partis politiques engagés dans la campagne des élections municipales, à laquelle plusieurs membres du RCPE, tels que VIGINUM et l'Arcom, ont pu intervenir pour présenter leurs actions respectives en matière de protection de l'intégrité des scrutins et les risques associés aux processus électoraux.

En outre, VIGINUM a mené une campagne de sensibilisation auprès des partis politiques et des équipes de campagne, à la fois en intervenant lors du congrès annuel de l'Association des Maires de France le 19 novembre 2025, et en publiant un guide de sensibilisation le 8 décembre 2025, lequel a été relayé par l'Arcom sur son site internet[4].

Pour aller plus loin…

Guide de sensibilisation à l'attention des équipes de campagne

1.3.2 Médias et grand public

Un plan de communication et de sensibilisation des autorités locales, des médias et des citoyens a été mis en œuvre à travers notamment la participation à des interviews et des articles, un point presse sur le nouveau dispositif de protection des élections et l'appui général de VIGINUM aux rédactions dans l'appréhension de ces sujets.

1.3.3 Plateformes

Dans le cadre de leurs missions respectives, plusieurs membres du RCPE développent des coopérations avec l'ensemble des acteurs de la lutte contre les manipulations de l'information, et notamment avec

[4] Cf. https://www.arcom.fr/temps-parole/election/municipales.

les fournisseurs de très grandes plateformes en ligne et moteurs de recherche (*Very large online platforms and search engines*, ci-après VLOPSEs[5]).

Afin de s'assurer d'une coordination efficace entre toutes les parties prenantes à la protection des élections, l'Arcom, en sa qualité de coordinateur pour les services numériques, a organisé une table ronde le 28 janvier 2026, réunissant plusieurs membres du RCPE et les autres services de l'État concernés, la Commission européenne, certains vérificateurs de faits ainsi que les représentants des principaux VLOPSEs opérant en France. Ces derniers ont pu présenter les mesures d'atténuation des risques liés aux élections qu'ils prévoyaient de mettre en place et ont pu être sensibilisés par VIGINUM, à cette occasion, au dispositif mis en place dans le cadre du RCPE. L'Arcom a également organisé une table-ronde post-électorale le 13 avril 2026 suivant le même format, dans l'objectif de dresser un bilan commun de la coordination de l'ensemble des acteurs concernés au cours de la période électorale.

[5] À titre d'exemples : *Facebook*, *Instagram*, *TikTok*, *X*, *YouTube*, *Google Search* ou *Microsoft Bing*.

2. Panorama des INE observées durant les élections municipales 2026

2.1 Tendances de la menace

2.1.1 Quatre stratégies de déstabilisation du débat public national en période électorale

En contexte électoral, les ingérences numériques étrangères font peser une menace réelle et sérieuse sur le fonctionnement démocratique des sociétés visées. Principalement mises en œuvre au moyen de modes opératoires informationnels (MOI) prépositionnés (cf. Lexique), elles ont pour objectif ou pour effet de déstabiliser le processus démocratique et les institutions chargées de l'organiser et de l'incarner. Cet objectif malveillant peut être atteint au travers de plusieurs stratégies, déjà observées par VIGINUM lors de précédents scrutins et décrites dans le premier bulletin d'information diffusé par le RCPE[6] :

- **la décrédibilisation de 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 ;
- **la polarisation du débat politique autour de thématiques clivantes** : cette stratégie consiste pour une puissance étrangère à amplifier de manière artificielle ou inauthentique la visibilité de certains sujets sensibles, susceptibles d'influencer les décisions des électeurs, afin de nourrir la polarisation du débat public et d'accroître ses divisions (politiques publiques, place des minorités, violences policières, débats religieux, *etc.*) ;
- **l'alimentation de la défiance vis-à-vis des médias du pays visé** : cette stratégie vise à délégitimer les médias (privés et publics) 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, susceptibles d'être administrées par des acteurs étrangers ;
- **l'exposition réputationnelle d'un candidat ou d'un parti politique** : cette stratégie a pour objectif de modifier la perception de l'opinion en dénigrant un candidat ou en le promouvant, à travers différentes tactiques, techniques et procédures.

Chacune des détections et caractérisations effectuées par VIGINUM sur la période des élections municipales de 2026 s'est insérée dans une ou plusieurs de ces quatre stratégies.

2.1.2 Entre persistance et évolution de la menace

L'analyse de la menace informationnelle étrangère durant la période électorale confirme plusieurs grandes tendances observées ces dernières années :

- **la persistance stratégique de certains acteurs étrangers malveillants,** qui cherchent à s'implanter durablement dans notre débat public numérique à travers le pré-positionnement d'écosystèmes et la conduite continue d'opérations au moyen de MOI connus de VIGINUM, détectés et exposés depuis plusieurs années. VIGINUM estime néanmoins que l'évolution du contexte international sur la période des élections municipales 2026, marquée par la persistance de conflits majeurs, la multiplication de crises au Proche et Moyen-Orient, et la tenue d'élections dans plusieurs pays d'Europe, a probablement mobilisé sur d'autres fronts certains des MOI suivis par VIGINUM ;
- **l'essor d'une économie de l'ingérence,** avec d'une part, l'émergence d'acteurs commercialisant des services d'intermédiation pour mener des ingérences numériques étrangères, et d'autre part,

[6] Cf. https://www.sgdsn.gouv.fr/files/files/Publications/20260130_SGDSN_RCPE_Bulletin d%27information n1-vd.pdf.

la multiplication d'INE à but lucratif diffusant des contenus présentés de façon sensationnaliste, afin de susciter de l'engagement et *in fine* générer des revenus ;

- **la clandestinisation croissante** des opérations d'INE, avec des acteurs cherchant à dissimuler leurs actions par l'utilisation de tactiques, techniques et procédures (TTP) diversifiées pour créer des écosystèmes plus complexes et mieux anonymisés.

2.2 Ingérences numériques étrangères observées durant les élections municipales de 2026

Sur la période de mise en place du RCPE, **quatre ingérences numériques étrangères** (INE) ciblant spécifiquement les élections municipales 2026 ont été détectées et caractérisées par VIGINUM. Une INE peut être constituée de plusieurs opérations informationnelles menée au moyen d'un même mode opératoire informationnel qui, ensemble, peuvent constituer une campagne[7]. Deux de ces INE ont été conduites au moyen de **MOI pro-russes connus** (*Storm-1516*, *CopyCop*, *Storm-1679* et *Matriochka*) qui avaient déjà mené des activités malveillantes contre la France dans le passé. Les deux autres INE ont été mises en œuvre au moyen de nouveaux modes opératoires informationnels détectés et caractérisés à l'occasion de ces élections municipales.

L'ensemble de ces opérations informationnelles ont été documentées par le RCPE dans le cadre des bulletins d'information publics diffusés chaque semaine sur le site du SGDSN[8].

2.2.1 Deux INE conduites au moyen de MOI pro-russes persistants

Une première INE mise en œuvre au moyen des MOI *Copy Cop* et *Storm-1516*

Depuis la fin de l'année 2023, VIGINUM suit et documente l'activité d'un mode opératoire informationnel pro-russe, connu en source ouverte sous le nom de *Storm-1516*. Attribué à l'unité 29155 du service de renseignement militaire russe (GRU) avec l'appui du *Centre d'expertise géopolitique,* officine d'influence moscovite, *Storm-1516* est un MOI particulièrement persistant et évolutif.

Capture d'écran d'un des faux sites d'information du MOI CopyCop

Les 205 opérations informationnelles qui lui sont imputables depuis août 2023 se sont en effet déroulées selon un schéma de diffusion en constante évolution, dont une partie importante repose sur une infrastructure numérique développée au moyen du MOI *CopyCop*, attribué en source ouverte à l'ancien policier américain exilé en Russie, John Mark DOUGAN. **Dans le cadre de la protection du débat public numérique lié aux élections municipales, VIGINUM a documenté une ingérence numérique étrangère composées de deux opérations informationnelles, imputées avec une confiance élevée à ces deux MOI.**

La première opération informationnelle, liée à *CopyCop* et lancée dès février 2025, a consisté en **l'enregistrement de plus d'une centaine de noms de domaine en « .fr » imitant des sites de presse locaux** et alimentés par des articles de presse reformulés par des outils d'intelligence artificielle générative. VIGINUM considère que certains de ces sites pré-positionnés dans l'écosystème informationnel

[7] Cf. https://www.sgdsn.gouv.fr/publications/definitions-et-objectifs-du-concept-de-mode-operatoire-informationnel-moi.
[8] L'intégralité de ces bulletins est disponible au lien suivant : https://www.sgdsn.gouv.fr/publications/bulletins-du-reseau-de-coordination-et-de-protection-des-elections.

francophone, et alimentés par des articles orientés et reformulés par IA, auraient pu être exploités par les opérateurs du MOI *CopyCop* pour cibler les élections municipales.

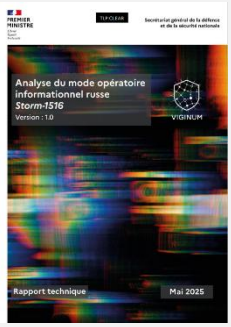
Cette opération informationnelle a été documentée par le RCPE dans ses bulletins d'information publics sur l'ensemble de la période pré-électorale, durant laquelle la campagne informelle est restée active. ***Elle n'a toutefois pas eu d'effet significatif,*** *la plupart des noms de domaine ayant été suspendus par l'Afnic*[9] *à l'issue d'une procédure de vérification d'identité des titulaires.*

La seconde opération informationnelle, conduite au moyen du MOI *Storm-1516*, a visé le candidat à la mairie de Paris, Pierre-Yves BOURNAZEL.

Cette opération a consisté en la diffusion d'un narratif affirmant que le candidat proposait de transformer le Centre Pompidou en un lieu d'accueil pour « tous les migrants sans domicile fixe » en 2030, et suggérait que plusieurs personnalités politiques françaises, dont le président de la République, soutenaient ce projet.

Le narratif a été primo-diffusé le 2 mars 2026, dans un article mis en ligne sur un site usurpant la charte graphique du site officiel du candidat, *macronavecbournazel.fr*, imputé par VIGINUM au MOI *CopyCop*. Il a ensuite été amplifié sur *X*, à partir du 4 mars 2026, dans une vidéo publiée par un groupe de comptes très probablement rémunérés par les opérateurs du MOI. Une partie de ces comptes avait déjà été identifiée par le passé comme des relais fréquents des opérations informationnelles conduites au moyen de ce MOI.

Pour aller plus loin…



Rapport sur le MOI Storm-1516

Cette opération informationnelle a été rendue publique par le RCPE dans son bulletin n°6 du 6 mars 2026[10]*, en indiquant que, si cette dernière visait à interférer dans le débat public national,* ***elle n'avait atteint qu'une audience limitée sur la période****, bien en-deçà du niveau de visibilité d'autres opérations du MOI ayant précédemment ciblé la France.*

Une seconde INE mise en œuvre au moyen des MOI *Storm-1679* et *Matriochka*

Entre janvier et mars 2026, VIGINUM a détecté sept opérations informationnelles imputées aux MOI *Storm-1679* et *Matriochka* [11], constitutives d'une ingérence numérique étrangère. Ces opérations ont consisté en la diffusion, sur les plateformes *Telegram* et *X*, de vidéos de faux reportages usurpant l'identité de plusieurs médias et institutions français pour prétendre que les élections ne pourraient pas avoir lieu dans de bonnes conditions de sécurité.

Capture d'écran d'une vidéo diffusée sur Telegram *au moyen du MOI* Storm-1679

Sur la plateforme *Telegram*, VIGINUM a détecté, le 9 mars 2026, la diffusion d'une vidéo usurpant le logo et l'identité du média français *20 Minutes*, prétendant que plus de la moitié des officiers de police parisiens aurait décidé de faire grève en amont des élections municipales françaises.

Sur la plateforme *X*, VIGINUM a détecté le même jour **six autres opérations informationnelles ciblant les élections municipales.** Ces opérations

[9] L'Afnic est l'*Association Française pour le Nommage Internet en Coopération*. Elle assure la gestion du registre des noms de domaine en France, en lien avec l'ensemble de l'écosystème de l'internet en France.
[10] Cf. https://www.sgdsn.gouv.fr/files/files/20260305_SGDSN_RCPE_Bulletin d%27information 6 VF.pdf.
[11] Le MOI *Storm-1679* consiste en la diffusion coordonnée, sur des chaînes *Telegram* russophones, de faux contenus usurpant fréquemment l'identité de médias et d'organisations. Certains de ces contenus sont ensuite amplifiés, sur *X*, *TikTok* ou encore *Bluesky*, au moyen d'un MOI distinct connu sous le nom de *Matriochka*.

consistaient en la diffusion de faux reportages usurpant l'identité des médias *BFM TV, RTL, Le Monde, NewsGuard et Euronews*.

Les narratifs diffusés par ces vidéos affirmaient respectivement que :

- les élections auraient été menacées en raison de la composition ethnique de la police en France, où 72 % des membres des forces de police seraient des descendants de migrants. Les « Français ethniques » restants seraient en majorité des soutiens du régime iranien ;
- les services de renseignement allemands auraient critiqué le prétendu transfert de la majorité des forces de police à Paris, qui laisserait les autres villes sans protection ;
- la Direction générale de la sécurité intérieure (DGSI) aurait exigé du Président de la République qu'il reporte la tenue des élections en raison du conflit au Moyen-Orient, qui augmenterait le risque d'attaques terroristes sur le sol français pendant le scrutin ;
- l'enregistrement de votants par procuration aurait drastiquement augmenté en France, où les personnes âgées et atteintes d'handicap auraient fait une procuration à des personnes inconnues , ce qui serait un signe de manipulation ;
- il aurait été ordonné à la police française de dissimuler les statistiques relatives aux crimes commis par les migrants en amont du scrutin ;
- un groupe de stratèges politiques arméniens serait secrètement arrivé en France avant les élections municipales pour gagner de l'expérience en « manipulation du vote ».

Pour aller plus loin…

Rapport de VIGINUM sur Matriochka

Le RCPE a rendu compte de ces opérations informationnelles dans son bulletin n°8 du 12 mars 2026[12], en estimant que ***leur risque d'impact sur le débat public numérique était considéré comme faible****, ces vidéos n'ayant obtenu qu'une audience relativement limitée et l'amplification observée sur X étant en grande partie artificielle.*

Par ailleurs, les activités malveillantes de ce MOI ayant été dénoncées publiquement à plusieurs reprises, elles ne font désormais que rarement l'objet d'une couverture médiatique, qui reste l'objectif principal des opérateurs.

2.2.2 Une INE à finalité lucrative conduite au moyen d'un nouveau MOI impliquant un acteur non-étatique localisé au Vietnam.

Au cours du mois de février 2026, VIGINUM a détecté l'activité d'un nouveau mode opératoire informationnel opérant depuis le Vietnam. Baptisé *Hydras Danbau*, ce MOI est formé par plusieurs centaines de sites internet et pages *Facebook* inauthentiques ciblant de multiples audiences dans le monde. Le service a notamment identifié **plus de 100 pages *Facebook* et 73 sites internet francophones impliqués dans la diffusion de contenus polarisants, centrés majoritairement sur l'actualité nationale française et internationale.** Générés par intelligence artificielle, les contenus publiés au moyen de ce MOI cherchent à instrumentaliser de façon opportuniste des événements d'actualité, des sujets de débat, ou des propos de personnalités politiques, en utilisant une approche polémique et alarmiste, voire en diffusant des narratifs inexacts ou trompeurs, afin de susciter l'engagement des internautes.

[12] Cf. https://www.sgdsn.gouv.fr/files/files/Publications/SGDSN_RCPE_Bulletin d%27information 8.pdf.

Les ingérences numériques étrangères à finalité lucrative

Au cours de l'année 2025, VIGINUM a pu observer et documenter la nette augmentation d'un phénomène déjà connu et identifié : l'exploitation et la diffusion, sur les plateformes numériques de contenus polarisants à des fins lucratives. Ces opérations témoignent d'un certain opportunisme de la part des acteurs étrangers les menant. En effet, la déstabilisation du scrutin n'est pas l'objectif recherché. Ces acteurs utilisent néanmoins un événement démocratique pour diffuser des contenus selon des modalités correspondant aux quatre critères de l'ingérence numérique étrangère.

L'objectif de ces acteurs est de générer de la visibilité et de l'engagement en mettant en avant des récits clivants, polémiques ou trompeurs, en vue de maximiser leur audience, et *in fine*, leurs revenus. Ces revenus peuvent être obtenus en exploitant les systèmes publicitaires programmatiques, en bénéficiant des programmes de redistribution de revenus aux créateurs proposés par les plateformes, ou encore par le biais de la revente des comptes.

Les thématiques choisies et modes de diffusion, qui visent à en maximiser la viralité, sont alors de nature à avoir un impact sur l'intégrité du débat public numérique. Ces dispositifs présentent ainsi tous les critères permettant de caractériser une INE, quand bien même leurs administrateurs ne seraient pas motivés par une volonté politique ou idéologique.

L'exacerbation des tensions géopolitiques, la multiplication des modèles d'intelligence artificielle (IA) générative, ainsi que le développement des fonctionnalités de monétisation sur les principales plateformes de réseaux sociaux ont néanmoins conduit ces dernières années à une accélération de ce phénomène déjà connu. Celui-ci est ainsi régulièrement documenté par différents acteurs de la lutte contre les manipulations de l'information, qu'il s'agisse d'associations ou de médias spécialisés.

La dimension lucrative de ce MOI repose sur la monétisation publicitaire des actifs numériques administrés par les opérateurs du MOI, notamment les sites internet promus par les pages *Facebook*, qui se présentent comme des blogs d'actualités ou des médias d'information. Les opérateurs du MOI s'appuient en effet sur la sponsorisation de publications pour inciter les internautes à s'abonner aux pages *Facebook*, qui diffusent quant à elles du contenu sensationnaliste comportant des liens de redirection vers des sites d'information comportant des emplacements publicitaires.

Schéma illustrant la mécanique à l'œuvre dans le cadre de cette opération d'INE

Entre le 1er janvier et le 31 mars 2026, **VIGINUM a plus particulièrement identifié 173 publications diffusées par les pages *Facebook* francophones du MOI faisant référence aux élections municipales de mars 2026, dans lesquelles plusieurs candidates et candidats de différents partis politiques ont été ciblés au moins une fois** (*La France Insoumise*, *Les Écologistes*, *Le Parti Socialiste*, *Les Républicains*, *Le Rassemblement National*, *Reconquête*).

Bien que leur visibilité ait été relativement limitée, certaines publications ont tout de même suscité plusieurs milliers, voire dizaines de milliers de mentions « j'aime ». Le ciblage des élections municipales par ce MOI semble résulter d'une logique opportuniste, les 173 publications représentant un volume marginal de l'activité globale de ce MOI durant cette période. VIGINUM a toutefois estimé que l'activité de ce MOI réunissait les critères d'une campagne d'ingérence numérique étrangère à but lucratif.

Plusieurs marqueurs techniques, tels que le nombre d'abonnés similaire, les éléments de biographie, les noms de page identiques, photos de profil générées par IA, **permettent d'affirmer le caractère inauthentique et coordonné** des pages *Facebook* qui forment ce MOI, notamment l'utilisation de la technique du *copy-pasta* (cf. Lexique) dans la diffusion de certains contenus et la présence de caractéristiques communes.

Captures d'écran de publications Facebook *instrumentalisant les élections municipales*

En outre, plusieurs contenus diffusés par ce MOI sont visiblement trompeurs. Une publication a notamment relaté un débat sur *BFM TV* entre les candidates Rachida DATI et Sarah KNAFO n'ayant jamais eu lieu.

Le MOI a également cherché à instrumentaliser des contenus extraits de certains débats entre candidats, parmi les plus médiatisés et de bords politiques opposés, accompagnés de narratifs polémiques, et en y associant des images ou citations provenant de contextes différents, afin de susciter l'engagement des internautes exposés à ces contenus.

Plusieurs éléments ont par ailleurs conduit VIGINUM à rattacher ce réseau de pages et de sites inauthentiques **à des opérateurs techniques vietnamiens** :

- selon les informations de transparence fournies par *Facebook*, la majorité des pages sont administrées depuis le Vietnam ;
- des marqueurs techniques indiquent que certains des sites inauthentiques d'information, développés avec *WordPress*, sont paramétrés sur le fuseau horaire de Hô Chi Minh-Ville ;
- selon les données de la bibliothèque publicitaire de *Meta*, certaines publications sponsorisées par des pages *Facebook* de ce MOI ont été financées par des entreprises de communication numérique vietnamiennes ;
- la plupart des administrateurs des sites et différents comptes ont des noms à consonnance vietnamienne, à l'instar de « *hailinh8386* », « *Nguyenlinh8386* », « *lananh8386* », qui finissent tous, par ailleurs, par la même suite de chiffres[13] .

Bien que les éléments techniques suggèrent que ce MOI semble principalement motivé par des objectifs lucratifs plutôt que politiques ou idéologiques, **il démontre une capacité à exploiter des sujets sensibles en période électorale, ce qui peut, par ricochet, déstabiliser le débat public national.** En effet, indépendamment des finalités recherchées, l'exposition des citoyens à des contenus clivants ou trompeurs est susceptible d'altérer leur perception du débat public numérique, et **cette distorsion est de nature à porter atteinte aux intérêts fondamentaux de la Nation.**

Les activités de ce MOI ont été rendues publiques par le RCPE dans le cadre de ses bulletins d'information n°5, 6, 8 et 9. Malgré la poursuite de la campagne sur plusieurs semaines, ***la majeure partie des pages ciblant les audiences francophones sur les plateformes numériques était devenue inaccessible****, limitant leur impact sur le débat public numérique français.*

[13] Cette combinaison de chiffres est notamment utilisée sur les réseaux sociaux par la jeunesse vietnamienne comme jeu de mots pour souhaiter « prospérité et fortune ».

2.2.3 Une INE ciblant des candidats du parti *La France Insoumise* conduite au moyen d'un nouveau MOI impliquant un acteur non-étatique localisé en Israël

En mars 2026, VIGINUM a détecté **une campagne informationnelle visant à dénigrer le parti politique *La France Insoumise*** (LFI) **ainsi que plusieurs de ses candidats aux élections municipales**, conduite par **un nouveau MOI** formé d'un réseau de plusieurs sites *web* et de comptes de réseaux sociaux. Ce MOI, baptisé *Rokh Solis,* a mené quatre opérations informationnelles qui réunissent les critères d'une ingérence numérique étrangère. Les trois premières opérations informationnelles ont consisté à dénigrer le parti politique LFI et certains de ses candidats : François PIQUEMAL, Sébastien DELOGU et David GUIRAUD, respectivement candidats aux élections municipales de Toulouse, Marseille, et Roubaix. Dans cette perspective, plusieurs actifs numériques les concernant directement ont été déployés *via* des sites et des avatars sur des plateformes comme *X* ou *Facebook*.

Actifs numériques du MOI	Cible	Narratif
Le site *blogdesophie.com, les comptes* X et *Facebook « Le Blog de Sophie »*	Sébastien DELOGU	Accusation de viol
Le site *delogupourpalestine.com*	Sébastien DELOGU	Présentation d'une lettre prétendument rédigée par le candidat LFI qui proposerait à la vente un calendrier mettant en scène des photos de sa personne dont certaines seraient dénudées, afin de « *consacrer la vente de [ses] photographies à un soutien direct en faveur de la population de Gaza* ».
Deux pages *Facebook* et le site *piquemalzero.com*	François PIQUEMAL	Accusation de pédophilie, de violence et de soutien envers les actes terroristes du Hamas, usurpation d'identité d'une association de protection de l'enfance
Deux pages *Facebook*	David GUIRAUD	Dénonciation des prises de positions propalestiniennes dans le cadre du conflit qui oppose Israël au Hamas

La quatrième opération informationnelle a consisté à tenter de polariser le débat public numérique autour de thèmes clivants, en particulier en accusant le parti LFI de communautarisme musulman, à travers le déploiement de deux écosystèmes numériques distincts :

- le premier écosystème s'inscrit autour d'un prétendu projet, « L'Alternative 2026 » : incarné par le site internet *lalternative2026.com*, faisant la promotion d'une démarche politique communautariste en faveur de la population musulmane dans le cadre des élections municipales, en citant une liste de candidats LFI présentés comme alignés avec ce programme communautariste. Une partie de cet écosystème a pour but de promouvoir ce projet *via* des actifs numériques empruntant le nom d'un ancien groupe radical islamiste dissous en 2012, « Forsane Alizza[14] », et véhiculant des narratifs inspirés du socle idéologique salafiste de ce groupe, et saluant l'initiative portée par *lalternative2026.com* ;

[14] *Forsane Alizza* ou « Cavaliers de la Fierté », était un groupe radical islamiste se présentant sous le statut d'une association depuis 2010. Le groupe était constitué d'une quinzaine d'individus actifs en France entre 2010 et 2012. Les activités de ce groupe se structuraient principalement autour d'actions en ligne et de manifestations dans la sphère physique, sur des thématiques essentiellement antisémites et anti-blasphématoires.

- le second écosystème antagoniste s'insère quant à lui au sein d'une doctrine souverainiste, identitaire, catholique et conservatrice. Ainsi, une prétendue association nommée « Renaissance catholique Nationale », *via* le site *rcn-france.org*, a pour mission de participer à la dénonciation de l'existence du site *lalternative2026.com*.

Le déploiement de l'ensemble de ces actifs numériques, ainsi que leur comportement et certaines mesures d'amplification, présentent de nombreux marqueurs de coordination et d'inauthenticité.

A gauche, capture d'écran du site lalternative2026.com, *à droite, celle du site* rcn-france.org ;
Ci-contre, capture d'écran du site forsane-alizza.eu

Concernant la structure du mode opératoire informationnel *Rokh Solis* :

- quatre des sites *web*[15] – ***blogdesophie.com***, ***delogupourpalestine.com***, ***piquemalzero.com*** et ***lalternative2026.com*** – présentent des **caractéristiques techniques communes.** Les sites *blogdesophie.com* et *lalternative2026.com* ont tous deux été déposés le 9 février 2026 sur l'adresse IP 198.177.120[.]194, sur laquelle est également hébergé le site *piquemalzero.com,* enregistré quant à lui le 11 février 2026. Le site *delogupourpalestine.com* est à son tour enregistré le 19 février 2026 sur l'adresse IP 198.177.120[.]196. Sur ce site, VIGINUM a identifié des métadonnées communes avec le site *blogdesophie.com*. ;
- les pages *Facebook* associées à ces sites, ainsi que celles ciblant spécifiquement David GUIRAUD, présentent également des caractéristiques communes. Celles-ci sont créées entre le 9 et le 19 février 2026, y compris pour le compte *X @LeBlogdeSophie0* créé le 18 février 2026. Ces actifs numériques servent à la diffusion de nombreux contenus ciblant les trois candidats précités, incluant, dans le cadre du « Blog de Sophie », la publication de photos exposant des collages de tracts dans les rues de Marseille ;
- une page *Facebook*, *@EnfanceetPartageorg*, usurpant l'identité d'une association de protection de l'enfance a été créée dans le but de diffuser des accusations de violence à l'encontre de François PIQUEMAL. Cette page possède également des caractéristiques communes avec les

[15] Cf. https://archive.ph/KebHZ ; https://archive.ph/O1CBf ; https://archive.ph/2TnzW ; https://web.archive.org/web/20260228175025/https://lalternative2026.com/.

pages mentionnées précédemment (création entre le 15 février et intégration au sein de groupes *Facebook* durant la même période que des comptes amplificateurs de l'opération, voir ci-dessous).

- les analyses réalisées sur le site *lalternative2026.com* ainsi que sur des comptes associés au MOI *Rokh Solis* permettent de rattacher deux autres sites à ce même écosystème : ***forsane-alizza.eu*** (affichant son soutien à *lalternative2026.com*), et ***rcn-france.org*** (qui, au contraire, alerte sur l'existence de *lalternative2026.com*). Le site *forsane-alizza.eu* a été enregistré le 14 septembre 2025 sur l'adresse IP 80.78.18[.]115, localisée en Suède. Plusieurs actifs numériques sur *Facebook* et *Instagram* déployés entre octobre 2025 et mars 2026, ont servi d'interface de prolongement de ce site[16]. Le site *rcn-france.org* est une redirection effectuée à partir du nom de domaine *rcn-france.com* enregistré le 26 mars 2025. Cet actif numérique est incarné sur *TikTok* par le compte *@renaissancecatholiquefr*, créé le 12 septembre 2024[17].

S'agissant des procédés d'amplification des principaux actifs numériques précités, VIGINUM a identifié plusieurs groupes de comptes inauthentiques opérant simultanément sur plusieurs plateformes :

- des groupes de comptes *Facebook a priori* vietnamiens, et dont l'apparence ne cherche pas à dissimuler le caractère inauthentique, ont diffusé de manière coordonnée des éléments techniques liés au MOI *Rokh Solis*. Le nom de domaine *piquemalzero.com* a été relayé sur une des publications du compte *Facebook* officiel de François PIQUEMAL le 6 mars 2026. Tandis que le *hashtag #forsannealizza* a été propagé dans les commentaires d'une publication de Julien ODOUL le 13 octobre 2025[18] ;
- un groupe d'avatars sur *Facebook*[19], présentant des comptes équivalent sur *X* et *Instagram,* a été déployé dans le but de relayer au sein d'autres groupes *Facebook* les contenus partagés par les principales pages du dispositif. Les caractéristiques de ces avatars sur *Facebook,* et leurs équivalents, montrent une recherche plus poussée de crédibilisation de ces profils par les opérateurs du MOI. Ce sont souvent des profils générés par IA, utilisant des noms francophones très répandus (Lea Leclerc, Julie Simon, Elise Martin, Claire Martin, Etienne Martin, Sophie Dupoint, Luc Dupont, *etc.*) et présentant des fils de publications identiques. Afin de cibler une audience francophone, ces comptes se sont coordonnés pour se prépositionner au sein d'une dizaine de groupes *Facebook*[20] autour du 7 septembre 2025 puis du 19 février 2026 ;
- concernant ce dernier point, VIGINUM a également identifié un lien direct entre ce groupe de comptes *Facebook* inauthentiques ayant visé les élections municipales et un groupe de comptes impliqués dans l'amplification artificielle de contenus gouvernementaux angolais ou de publications faisant la promotion du parti présidentiel de João LOURENCO. Ces comptes possèdent les mêmes caractéristiques (photos de profil générées par IA, noms lusophones très répandus, fils de publications identiques) et ont vu plusieurs de leurs publications être amplifiées par certains comptes du groupe ayant visé les élections municipales françaises.

---

[16] Voir le groupe « Forsane Alizza » https://archive.ph/xK0Yo ; la communauté « Forsane Alizza » et le compte « Forsane Alizza », anciennement appelé « Manon Berger », probablement issus d'un groupe de comptes *Facebook* destiné à l'amplification du dispositif ; (https://*web*.archive.org/*web*/20260307132620/https://www.facebook.com/login/?next=https%3A%2F%2Fwww.facebook.com%2Fforsanealizza).

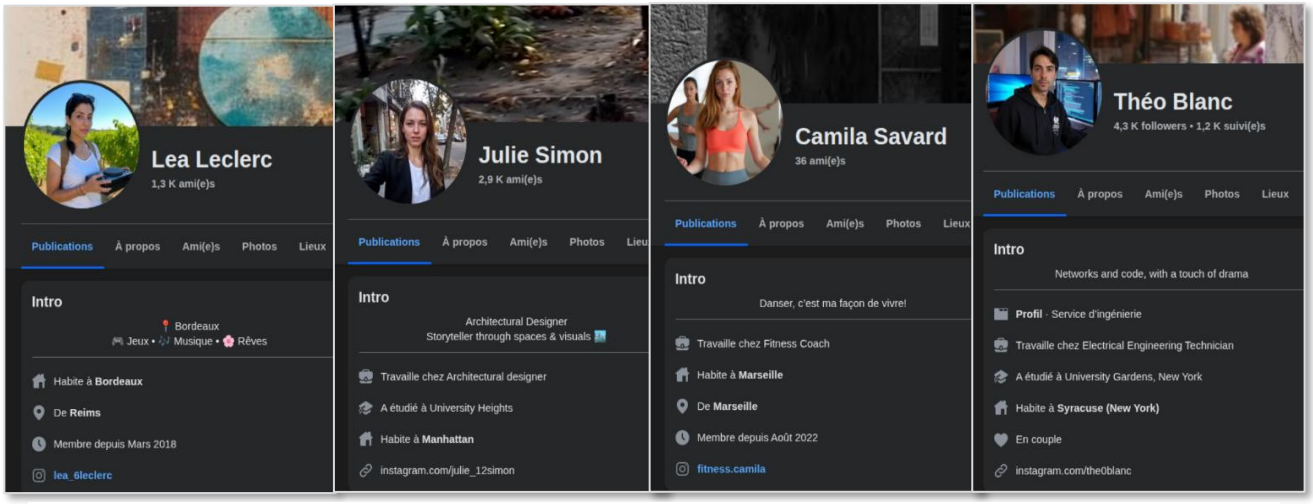
[17] Entre septembre 2024 et août 2025, le compte *TikTok @renaissancecatholiquefr* s'est mobilisé pour promouvoir le *hashtag* pro-israélien *#TheWestIsNext* et des narratifs islamophobes ciblant une audience anglophone. Il est par la suite renommé en août 2025 et est redirigé vers la diffusion de narratifs souverainistes ciblant l'audience francophone.

[18] Cf. https://facebook[.]com/reel/2423327021466972. ; https://archive.ph/aQxey.

[19] Cf. https://archive.ph/DjYUV ; https://archive.ph/p1X5u ; https://archive.ph/2dnnW ; https://archive.ph/Lmd75

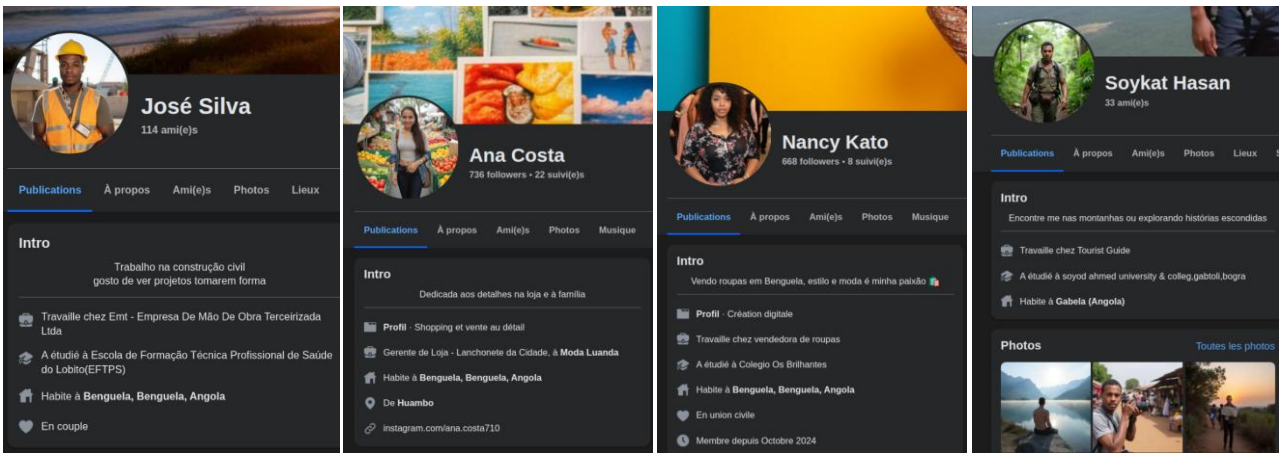
[20] Cf. https://archive.ph/1K5sA. ; https://archive.ph/pL4bD

- un groupe de comptes *Facebook* inauthentiques, se présentant la plupart du temps sous la forme de profils masculins générés par IA et créés la plupart du temps le 11 ou le 12 février 2026, était destiné à la diffusion de commentaires sous les publications des principaux actifs numériques du MOI. Entre le 19 et le 28 février 2026, 138 utilisateurs uniques ont été identifiés dans la publication de 338 commentaires sur ces différentes pages (« Le Blog de Sophie », « Qui est Sébastien Delogu ? » et « Je suis François Piquemal et je ne suis rien »).



Ci-dessus : exemples d'avatars issus du deuxième groupe de comptes Facebook *amplifiant le MOI* Rokh Solis

Ci-dessous : exemples de comptes issus du cluster ciblant l'Angola sur Facebook



Enfin, s'agissant de l'**implication d'un acteur étranger**, VIGINUM a relevé plusieurs **marqueurs techniques d'extranéité liés aux actifs numériques du MOI *Rokh Solis* :**

- **la présence de caractères hébreux** dans les métadonnées de *lalternative2026.com*. Le nom d'utilisateur *Canva* utilisé pour le site *forsane-alizza.eu* comporte des caractères hébreux et indique une localisation en Israël ;
- **plusieurs comptes** participant aux manœuvres d'amplification des contenus issus des principaux actifs du MOI *Rokh Solis*, **indiquaient des localisations en Israël**. C'est le cas du compte *TikTok @renaissancecatholiquefr*, ou au sein du deuxième groupe d'avatar *Facebook* pour « Amélie Charpentier » et « Maxime Meireles » respectivement renommés « Shirel Matana » et « Romi Shushan »[21] ;

[21] Cf. https://archive.ph/5BYtq. https://archive.ph/q059Z.

- la diffusion de *hashtags #TheWestIsNext* ou *#TheWestIsNow* [22] par le compte *TikTok @renaissancecatholiquefr* ainsi que le partage de publications associées à l'organisation pro-israélienne ELNET par des groupes de comptes inauthentiques sur *Facebook* et *X*[23].

Sur la base de la connaissance du service et des éléments techniques caractérisés, VIGINUM estime que le MOI *Rokh Solis* pourrait présenter des caractéristiques communes avec l'activité d'une entreprise israélienne œuvrant dans le domaine de l'influence, nommée *Blackcore*. Les investigations conduites sur cette dernière ont en effet permis de caractériser une infrastructure *web* liée à cette pseudo-entreprise délivrant des solutions d'influence en ligne, *via* notamment l'amplification artificielle de contenus et la conduite d'opérations informationnelles clandestines. À ce stade des analyses, aucun élément ne permet toutefois à VIGINUM d'établir l'identité et l'origine des commanditaires ayant pu recourir aux services de cette société.

Blackcore n'est *a priori* pas inscrite au registre des entreprises israéliennes mais possède tout de même un nom de domaine, *blackcore.online*, enregistré le 22 août 2025 ainsi qu'un compte *LinkedIn*, *@officialblackcore*. Plusieurs sous-domaines[24] associés à *blackcore.online* donnent quelques précisions sur les stratégies employées par l'entreprise pour mener des opérations d'influence. Parmi ces sous-domaines, l'un d'entre eux[25]explicite le programme d'une formation en communication numérique dispensée par *Blackcore* auprès du gouvernement angolais .

Un autre sous-domaine[26] est relié à un large éventail d'outils d'amplification artificielle, renvoyant vers d'autres entités, qui ne présentent *a priori* pas d'existence légale. Ces dernières indiquent cependant plusieurs liens techniques avec les sites *galacticos.ai* appartenant à la société *Galacticos LTD*, domiciliée à Tel Aviv[27]. Guy GEYOR et Doron AFIK, tous deux citoyens israéliens ont fondé et/ou dirigé cette entreprise. Doron AFIK dirige également la société d'avocat *Afik & Co*, domiciliée à la même adresse que *Galacticos*.

Dans un article publié sur le site d'*Afik & Co*, Yigal UNNA, citoyen israélien et ancien dirigeant de l'*Israel National Cyber Directorate* (*INCD*), est présenté lors d'un rassemblement diplomatique comme étant un représentant de *Galacticos*. De plus, la société israélienne dirigée par Yigal UNNA, *Cygun*, affiche le logo de *Galacticos* sur une page de son site *web*[28] présentant les différentes s*tart-ups* que la société soutient. L'article d'*Afik & Co* a également été diffusé sur le compte *LinkedIn* d'*Afik & Co*. Cette publication a fait l'objet de réactions issues d'un réseau d'une trentaine de comptes aux caractéristiques inauthentiques ayant également réagi à l'unique publication du compte *LinkedIn* de *BlackCore*.

Enfin, un autre sous domaine relié au site de *Blackcore* renvoie à la société *Iron Mind* spécialisée dans le développement de logiciels. Cette dernière a été fondée par Nir DOBICKY, habitant en Suède et d'origine israélienne, à la tête de plusieurs sociétés œuvrant dans le domaine de l'influence en ligne.

---

[22] Ce slogan fait partie des récits diffusés et promus par des sphères pro-israéliennes à partir d'octobre 2023, à destination d'audiences occidentales, présentant Israël comme le seul rempart contre le Hamas, dont l'Europe et l'Occident seraient les prochaines cibles.

[23] Exemple sur *Facebook :* https://archive.ph/BvZcd. ; comptes *X :* *@ErnestEnchelom*, *@Adrienubois*, *@AlexandrMoreau*, *@AmeliCharpente*, *@LeaaaLeclerc*, *@manon_bergers*, *@Theo0Blanc*, *@Celinejtaime*, *@EscofilPericles*. Ces derniers ont également publié des réponses sous une publication *X* du média *Sud Radio* traitant du sujet de *lalternative2026.com*. Cf. https://archive.ph/QbM1m ; https://archive.ph/UNDV7.

[24] https://archive.ph/WQA4N ; https://archive.ph/vRSAo.

[25] *angola-plan.blackcore.online.*

[26] p*roposals.blackcore.online* est hébergé sur la même adresse IP que les noms de domaines *electric-marinade.com* et *omrisystems.com.*

[27] 103 Hachashmonaim à Tel Aviv.

[28] *cygun.col.il*.

En outre, grâce aux investigations conduites sur l'infrastructure *web* autour des sous-domaines liés au site de *Blackcore*, VIGINUM a détecté des traces d'une autre campagne ciblant une audience pro-palestinienne autour du site *sadaqahpalestine.com*. ayant fait la promotion d'une pseudo-organisation caritative au profit de la population palestinienne nommée « Sadaqah Palestine ».

L'analyse de l'activité du compte *X @sadaqahpalestin* relié au nom de domaine cité *supra*, a révélé l'existence d'un groupe de comptes participant à l'amplification de ses publications. Celles-ci ont toutes bénéficié de la publication de commentaires par des comptes dont les caractéristiques présentent de nombreux marqueurs d'inauthenticité et un comportement identique aux comptes identifiés dans les commentaires des contenus présents sur les pages *Facebook* ciblant Sébastien DELOGU, François PIQUEMAL et David GUIRAUD. Or, ces comptes sont également présents dans les commentaires de certaines publications du compte *X* de Nir DOBICKY, *@niroknox*.

De surcroît, l'exploitation du logo présent sur le compte *X @sadaqahpalestin* a permis d'identifier sur la plateforme *Fiverr*, le profil « paullussac », qui serait à l'origine d'une demande de prestation pour la création de ce logo. Ce même profil a également des avis renvoyant à des outils de génération de vidéos par intelligence artificielle qui seraient destinés à des audiences togolaise ou gabonaise[29].

Enfin, VIGINUM a relevé la présence du numéro de téléphone (+972549729306), sur le site *sadaqahpalestine.com*. Celui-ci est relié à un compte *TikTok, @deepdiveafrica* indiquant une localisation en Israël. Tandis qu'une publication de *@deepdiveafrica* fait la promotion de l'ouverture d'un hôpital israélien au Togo à des fins humanitaires, une autre de ses publications affiche un logo sur lequel est inscrit « Politizando Angola ». Par ce biais, VIGINUM a identifié une page *Facebook* inactive « Politizando Angola » s'étant intégrée dans les mêmes groupes que ceux identifiés pour les comptes *Facebook* inauthentiques promouvant les contenus pro-gouvernementaux angolais.

L'identification de liens techniques entre ces opérations et l'infrastructure *web* de *Blackcore,* permet, notamment par les procédés d'amplifications détectés, de rattacher ces éléments aux MOI *Rokh Solis* et les opérations d'ingérence numérique étrangère analysées dans le cadre des élections municipales en France.

Le RCPE a partagé l'état des investigations de VIGINUM sur ce MOI dans les bulletins d'information n°7, 8 et 9. ***Malgré les nombreuses tentatives d'amplifications mises en œuvre par ce MOI, la visibilité des différents contenus diffusés durant la campagne électorale est restée limitée.*** *Par ailleurs, VIGINUM a constaté que, suite au dévoilement de cette campagne par la presse le 9 mars 2026, puis en mai 2026 plusieurs actifs numériques de ce MOI ont été supprimés, et l'activité du MOI a significativement ralenti.*

[29] Un autre de ses avis renvoie également vers la création d'un site internet pour une société localisée en Israël, *twostepinnovations.com*, hébergé sur les mêmes adresses IP que *blackcore.online*.

3. Synthèse de l'action du RCPE et mesures d'atténuation de la menace

3.1 Appréciation de la menace détectée et caractérisée

Lors de ses réunions, le RCPE s'est attaché à apprécier le niveau de menace d'ingérence numérique étrangère pesant sur le scrutin sur la base des détections et caractérisations de VIGINUM, afin d'éclairer la prise de décision du SGDSN dans le choix des mesures de réponses les plus appropriées. Cette appréciation s'est fondée sur une approche visant à évaluer la visibilité des opérations détectées, ainsi que leur potentiel risque d'impact sur l'information des citoyens, et plus largement sur le débat public numérique.

3.1.1 De la difficulté d'évaluer les effets d'une ingérence numérique étrangère sur le débat public numérique

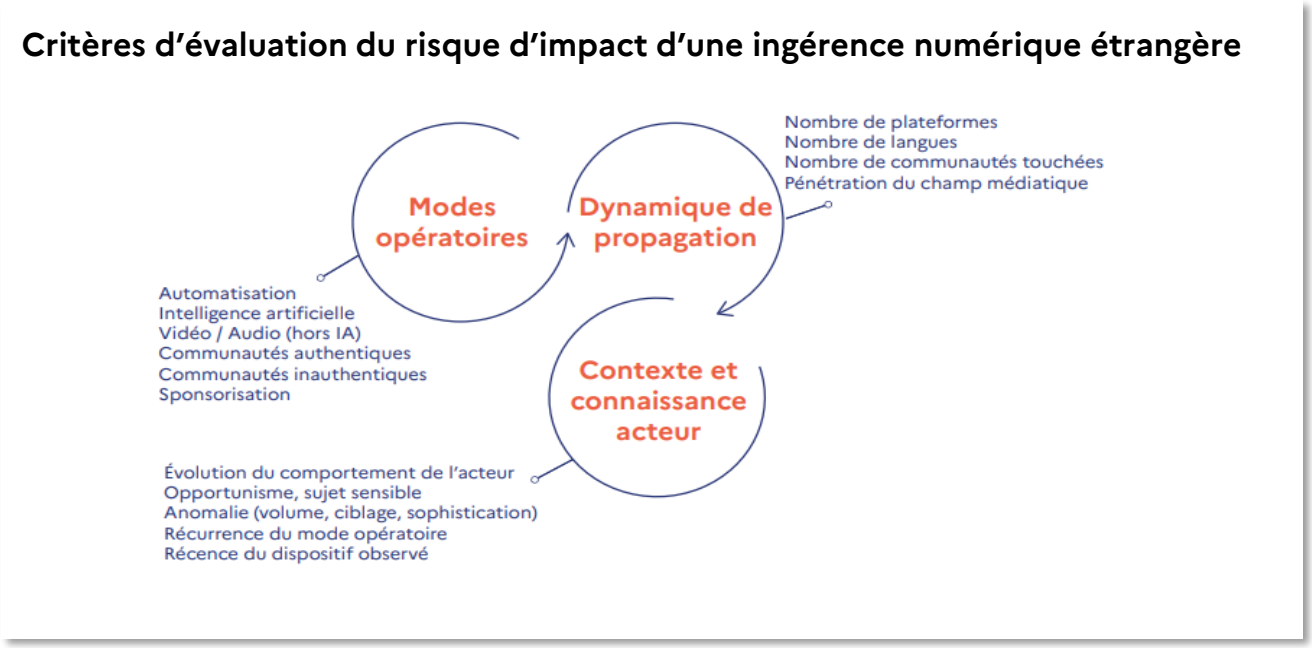
La question de la mesure d'impact ou du risque d'impact d'une opération d'ingérence numérique étrangère constitue un défi majeur pour les acteurs engagés dans la lutte contre les manipulations de l'information. En effet, l'objectif est de dépasser une lecture limitée aux indicateurs de visibilité (vues, *likes*, *etc*.) offerts par les plateformes - et dont la fiabilité ne peut être contrôlée - pour s'intéresser à l'analyse des effets notamment sociologiques, politiques, ou économiques, susceptibles d'être engendrés, de manière volontaire ou non, par ces INE. Évaluer leur risque d'impact suppose nécessairement de la prudence et une approche combinant des indicateurs quantitatifs et qualitatifs variés. Cette estimation est capitale, d'une part parce qu'elle permet de mieux comprendre les ressorts sur lesquels reposent les ingérences numériques étrangères et, d'autre part, parce qu'elle permet de déterminer des seuils de criticité essentiels pour concevoir et piloter une stratégie de réponse adaptée.

Pour ce faire, le RCPE s'est appuyé sur un outil méthodologique développé par VIGINUM, baptisé VIGISCORE, dont l'objectif est d'estimer rapidement le risque d'impact d'une INE détectée.

Le **VIGISCORE** s'inspire de différents travaux et recherches existants sur le sujet[30]. Il repose à la fois sur la description objective des différents éléments techniques observés, sur la dynamique de propagation cross-plateformes et cross-communautés de l'opération d'INE, et sur une appréciation de son caractère novateur et du contexte politique et social dans lequel elle s'inscrit. En croisant les caractéristiques techniques et les seuils de viralité, le VIGISCORE vise à fournir une évaluation anticipée du risque d'impact d'une opération d'INE dès sa détection.

Cette approche est adaptable à tous types d'acteurs, de modes opératoires et de temporalités. En fournissant des éléments d'évaluation plus approfondis que la simple analyse des métriques et des indicateurs de « performance » fournis par les plateformes, elle permet une meilleure qualification des INE observées en appréciant leurs capacités à produire un impact dans le débat public numérique.

[30] En particulier, la « Breakout Scale » de Ben NIMMO (2020) et l'« Impact Risk Index » de l'ONG *EU DisinfoLab* (2022, mis à jour en 2025). Cf. https://www.brookings.edu/articles/the-breakout-scale-measuring-the-impact-of-influence-operations/ et https://www.disinfo.eu/publications/updating-the-eu-disinfolab-impact-risk-index-addressing-ai-and-coordinated-inauthentic-behavior/.



3.1.2 Une visibilité limitée des INE détectées durant la campagne électorale

Se fondant sur l'analyse des données collectées et en prenant en compte les précautions mentionnées *supra*, les membres du RCPE estiment que les différentes opérations détectées et caractérisées n'ont eu qu'une visibilité limitée, ainsi qu'un impact qualifié de faible sur le débat public numérique national durant la campagne électorale. Ceci s'explique notamment, d'une part, par le fait que la plupart de ces opérations ne sont pas parvenues de manière organique à sortir de leur réseau inauthentique d'origine, et, d'autre part, par l'efficacité des mesures d'atténuation mises en place par le RCPE (cf. *infra*).

Par ailleurs, il est probable que l'augmentation du volume d'informations liées à l'actualité internationale et politique (conflits en cours et ouverture d'une nouvelle crise au Proche et Moyen Orient) ait mécaniquement diminué les capacités, pour un acteur étranger malveillant, de se rendre visible au cours de la période électorale.

Toutefois, il convient de préciser que si le RCPE a procédé à une évaluation de la visibilité et du risque d'impact de ces opérations sur l'information des citoyens, cette analyse ne peut être confondue avec l'évaluation de leurs effets réels sur les opinions et les intentions de vote. Il est rappelé ici que l'appréciation de l'impact sur la sincérité du scrutin relève exclusivement de la compétence du juge de l'élection en cas de contentieux post-électoral, et ne constitue pas une mission dévolue au RCPE.

3.2 Réponses et mesures d'atténuation mises en œuvre

Lors des réunions du RCPE, après avoir analysé et évalué le risque d'impact des opérations détectées, ses membres ont pu échanger et statuer sur les actions de réponse et mesures d'atténuation susceptibles d'être décidées par le SGDSN puis mises en œuvre par les entités compétentes. Ces actions ont reposé sur les différents leviers à disposition du réseau : information des acteurs ciblés, communication publique et coopération avec les fournisseurs de plateformes en ligne et moteurs de recherche.

3.2.1 L'information des acteurs victimes d'opérations d'ingérence numérique étrangère

Les acteurs victimes, qu'il s'agisse des équipes de campagne et partis politiques des candidats visés (*Reconquête, Les Républicains, La France Insoumise, le Parti Socialiste, Horizons, Les Écologistes,* et le

Rassemblement National), ou des médias dont l'identité a été usurpée (*RTL, Le Monde, BFM TV, 20 Minutes, NewsGuard* et *Euronews*), ont systématiquement été informés par le SGDSN de l'existence d'une INE visant à les déstabiliser. Cette information est intervenue avant chaque publication du bulletin d'information mentionnant ces INE.

3.2.2 Une communication transparente et régulière

Considérant que **la meilleure protection contre ces INE est l'information des citoyens,** le RCPE a communiqué de manière transparente afin d'éclairer le débat public, et d'entraver les stratégies déployées par les opérateurs étrangers malveillants.

Comme précédemment évoqué, des bulletins d'information du RCPE[31] ont été publiés chaque semaine sur le site du SGDSN, afin de rendre compte de l'état de la menace observée. Les bulletins ont par ailleurs été systématiquement transmis à la presse et aux médias (presse quotidienne régionale, presse écrite nationale, télévision, radio…). Une cinquantaine d'articles et de reportages ont été publiés, contribuant à l'information et à la sensibilisation du grand public.

En révélant les caractéristiques et les finalités des INE détectées, ces expositions publiques ont contribué à atténuer la menace, à la fois parce qu'elles ont participé à élever le niveau de vigilance du public, mais également parce que ces mises en lumière ont conduit, pour certaines, à l'arrêt des opérations par leurs opérateurs.

3.3.3 La coopération avec les fournisseurs de très grandes plateformes en ligne et moteurs de recherche

Des actions de coopération avec les plateformes en ligne ont également été mises en œuvre par les membres du RCPE compétents dans ce domaine : l'Arcom et VIGINUM.

L'Arcom a déployé un plan d'actions en partie destiné à l'accompagnement des principaux VLOPSEs opérant en France[32], en raison de leur place centrale dans le débat public et des risques qu'ils peuvent présenter pour l'intégrité des scrutins. Elle a adopté des préconisations à leur attention le 7 janvier 2026, afin de les guider dans la mise en œuvre de mesures visant à protéger les élections, et a organisé une série de rencontres avec eux, fondées sur leur participation volontaire (une réunion multilatérale avec l'ensemble des VLOPSEs, deux séries de réunions bilatérales avec chacun d'entre eux[33] et des table-rondes pré et post-électorales avec les membres du RCPE, les autres autorités et administrations compétentes ainsi que les vérificateurs de faits). L'Arcom souligne l'importance de procéder à ces échanges avec les VLOPSEs, afin de pouvoir utilement suivre et apprécier l'état de la menace informationnelle, ainsi que les moyens qu'ils mettent en place pour y faire face[34].

Dans le prolongement de sa mission de détection et de caractérisation des ingérences numériques étrangères, VIGINUM a également mis en œuvre une logique de coopération de long terme avec l'ensemble des acteurs externes occupant un rôle central dans la lutte contre les manipulations de l'information, y compris les VLOPSEs.

Pour aller plus loin…

Secrétariat général de la défense et de la sécurité nationale

Réseau de coordination et de protection des élections

26 mars 2026 | n° 10

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

Bulletins du réseau de coordination et de protection des élections

[31] Cf. https://www.sgdsn.gouv.fr/publications/bulletins-du-reseau-de-coordination-et-de-protection-des-elections.

[32] *Google Search, YouTube, Meta* pour *Facebook* et *Instagram, X, TikTok, LinkedIn, Snapchat* et *Wikimédia* pour *Wikipédia.*

[33] À noter que la plateforme *X* a décliné la proposition de l'Arcom et que *Wikimédia* n'a pas souhaité réitérer l'exercice une seconde fois en l'absence de menace significative sur son service.

[34] L'ensemble des moyens et mesures déployés par les VLOPSEs pendant les élections municipales sont détaillés dans le rapport sur la campagne en vue des élections municipales (15 et 22 mars 2026) de l'Arcom.

Conformément à l'approche opérationnelle de VIGINUM, cette coopération repose notamment sur le partage d'éléments techniques relatifs aux opérations caractérisées, et en particulier leurs marqueurs d'inauthenticité, de manière agnostique quant aux contenus et narratifs diffusés[35]. Les résultats obtenus grâce à ces échanges techniques mis en place par le service avec certains fournisseurs ont ainsi démontré qu'une coopération était mutuellement bénéfique face aux INE, qui contreviennent à leurs conditions générales d'utilisation et constituent un risque systémique au sens du Règlement sur les services numériques (RSN, en anglais *Digital Services Act*, DSA).

Durant la période électorale, VIGINUM a ainsi systématiquement communiqué aux fournisseurs des éléments techniques relatifs à l'activité de modes opératoires informationnels détectés et caractérisés, ciblant spécifiquement les élections municipales. Ces échanges ont permis à plusieurs fournisseurs de VLOPSEs d'identifier des comptes, pages ou chaînes administrés par des acteurs étrangers ciblant le débat public numérique français. Si l'ensemble des fournisseurs a été réactif face à ces remontées d'informations, VIGINUM salue la coopération avec ceux qui se sont montrés particulièrement proactifs, tels que *Google, Meta* et *Microsoft*, tant en matière de partage d'informations permettant de détecter et caractériser les ingérences numériques étrangères ciblant le scrutin, que dans les actions de modération à l'encontre des comptes, chaînes ou pages impliqués.

Dans le cadre de cette coopération essentielle avec les acteurs du numérique, **près de 200 pages, comptes et sites *web* inauthentiques ont été rendus inaccessibles dans des délais rapides, atténuant *de facto* l'impact potentiel de ces INE sur le scrutin.**

[35] Cf. https://www.sgdsn.gouv.fr/files/files/Publications/VIGINUM_rapport_activit%C3%A9_24_vd.pdf.

4. Bilan et grands enseignements pour 2027

Bien que le volume et l'impact des ingérences numériques étrangères détectées durant les élections municipales 2026 soient restés très limités, les opérations observées confirment **une volonté persistante de la part de certains acteurs étrangers de peser sur les processus électoraux nationaux.**

À l'évidence, l'élection présidentielle de 2027 constituera un rendez-vous politique et démocratique majeur dans un environnement international sous tensions et crises. Entre persistance et émergence de nouveaux acteurs et phénomènes, **une accentuation de la menace d'ingérence numérique étrangère est donc à anticiper pour ce scrutin**, que celle-ci soit destinée à servir les objectifs stratégiques de nos compétiteurs, ou bien qu'elle résulte d'une recherche de profit en instrumentalisant le débat public national.

Ces constats appellent donc à une vigilance accrue et au maintien des dispositifs de protection des élections contre les ingérences numériques étrangères et soulignent la pertinence de la mise en place d'un dispositif neutre, transparent et disposant de moyens d'action réactifs.

4.1 Réactivité opérationnelle du dispositif

Le RCPE a prouvé son efficacité pour apprécier rapidement la menace d'ingérence numérique étrangère et faciliter la prise de décision sur les mesures de réponse. Pour chaque détection d'une ingérence numérique étrangère susceptible d'altérer l'information des citoyens pendant la période électorale, les membres du réseau ont ainsi apprécié la situation et l'opportunité d'activer différents leviers de réponse : information des équipes de campagnes, mobilisation des institutions chargées du bon déroulement des élections, dénonciation publique de l'ingérence, voire la saisine de l'autorité judiciaire.

Dans la perspective d'un niveau de menace potentiellement supérieur lors des futures échéances électorales de 2027, le renforcement de la protection du débat public national passera par une organisation garantissant **une coopération inter-administrations et interministérielle renforcée**.

4.2 Intérêt de la coordination préalable avec les acteurs politiques et médiatiques

Les travaux amont de coordination avec les partis politiques et les médias ont contribué à renforcer la protection du débat public durant la période électorale.

D'une part, au-delà des retombées presse qui ont contribué à sensibiliser le grand public et à augmenter la résilience de la société, **différents médias ont également pu jouer un rôle à leur niveau dans la détection et de la caractérisation des INE.**

Par ailleurs, VIGINUM observe que la plupart des médias sont vigilants face aux menaces informationnelles, et ont montré de la retenue dans le traitement médiatique de certaines des opérations caractérisées afin de ne pas en amplifier la visibilité.

EXCLUSIF. Face au risque d'attaque numérique par des puissances étrangères, Viginum publie un guide pour les municipales

Attention danger, met en garde Viginum, l'organisme public créé en 2021 pour détecter les attaques numériques faites par des puissances étrangères. Il publie un guide ce lundi 8 décembre 2025. Entretien avec son chef de service, Marc-Antoine Brillant, et son adjointe, Anne-Sophie Dhiver.

Ouest-France
Patrice Moyon
Modifié le 07/12/2025 à 18h27
Publié le 07/12/2025 à 08h00

Abonnez-vous

LIRE PLUS TARD

PARTAGER

Newsletter La Matinale
Chaque matin,

Anne-Sophie Dhiver et Marc-Antoine Brillant, respectivement cheffe de service adjointe et chef de service de Viginum | CHIRET-FRANCE

Exemple de couverture presse

D'autre part, le choix, en coordination avec les partis politiques, de les informer directement d'une ingérence numérique étrangère les ciblant, s'est pleinement inscrit dans les principes d'impartialité, d'objectivité, de neutralité et de transparence guidant le RCPE. **Alors que l'un des objectifs des acteurs de la menace est de miner la confiance envers les institutions, cette démarche a prouvé sa validité et renforcé la légitimité du dispositif.**

4.3 Vertu de la régularité et de la périodicité de la communication

Chaque réunion du RCPE a fait l'objet d'un bulletin d'information public, accessible sur le site du SGDSN[36]. Cette communication a permis de créer une habitude qui a contribué à la sensibilisation de l'ensemble de la société et l'atténuation du risque de surréaction médiatique.

En vue des prochaines échéances électorales, **une stratégie de communication plus globale et proactive sera nécessaire afin de toucher une plus large audience et d'armer encore davantage la société contre les menaces informationnelles** et ainsi de renforcer sa résilience.

Enfin, si la société civile semble aujourd'hui plus vigilante face aux menaces informationnelles, **le risque d'augmenter la visibilité d'une opération informationnelle par son exposition publique demeure un véritable enjeu de la réponse.** En effet, la décision de communiquer sur une ingérence numérique étrangère peut s'avérer contre-productive en donnant de la visibilité et donc une empreinte dans l'opinion à des INE qui n'en avaient pas jusqu'alors. En déployant des manœuvres parfois peu sophistiquées, certains acteurs malveillants ont même pu rechercher à être repérés par des communautés expertes afin de susciter des publications, véritable indicateur de performance auprès de leurs bailleurs de fonds et/ou commanditaires. Ainsi, le choix de rendre publique une INE ou une opération informationnelle en temps réel repose sur une analyse recoupée du risque d'impact, c'est-à-dire de la probabilité que celle-ci puisse sortir des communautés de réseaux sociaux pour gagner la vie réelle.

4.4 Efficacité de l'atténuation des risques en lien avec les fournisseurs de plateformes en ligne

La coopération développée par VIGINUM et l'Arcom avec les fournisseurs de très grandes plateformes en ligne et moteurs de recherche (VLOPSEs) est apparue précieuse pour la protection du débat public numérique.

Toutefois, si le RCPE souligne la participation des VLOPSEs aux échanges engagés par les autorités et administrations compétentes, l'Arcom observe que ces derniers (représentés par leurs équipes d'affaires publiques lors des réunions organisées par le régulateur) ont manifesté des niveaux de coopération inégaux, et que certains n'ont fourni que des informations relativement peu détaillées sur l'état de la menace informationnelle observée et les dispositifs mis en œuvre pour protéger les scrutins.

De ce fait, cette coopération devra nécessairement être largement renforcée en amont de l'élection présidentielle de 2027, notamment en :

- formalisant davantage les canaux de coopération, notamment opérationnels, avec l'organisation d'échanges réguliers avec les équipes opérationnelles des fournisseurs ;
- partageant plus proactivement des éléments techniques relatifs à des comptes, pages ou chaines liés à des modes opératoires informationnels ciblant le débat public français ;
- mettant à disposition un réel accès aux données, notamment aux registres et APIs publicitaires comme le prévoit la réglementation européenne, afin de permettre aux équipes de VIGINUM de suivre l'activité de MOI déployés sur leurs services.

VIGINUM continuera d'exposer publiquement des modes opératoires informationnels opérés par des acteurs étrangers sur les plateformes en ligne et de faire remonter aux fournisseurs des éléments techniques sur les comptes, chaînes ou pages impliqués dans des opérations informationnelles et dont l'activité est contraire aux conditions générales d'utilisation des plateformes.

[36] Cf. https://www.sgdsn.gouv.fr/publications/bulletins-du-reseau-de-coordination-et-de-protection-des-elections.

En parallèle, **VIGINUM poursuivra sa participation à la mise en œuvre du Règlement sur les services numériques (DSA) de l'Union européenne** en transmettant à l'Arcom tout élément utile pour documenter les potentiels manquements des fournisseurs à leurs obligations d'atténuation des risques systémiques, et ce, particulièrement pour les plateformes dont l'absence de coopération témoigne de leur manque de volonté à mettre pleinement en place des mesures d'atténuation suffisantes.

5. Lexique des ingérences numériques étrangères

5.1 Typologie de la menace informationnelle

Ingérence numérique étrangère : volet numérique de la manipulation de l'information, elle consiste pour un État étranger ou une entité non-étatique étrangère, à diffuser de manière artificielle ou automatisée, massive et délibérée des contenus manifestement inexacts ou trompeurs, susceptibles de porter atteinte aux intérêts fondamentaux de la Nation.

Malinformation : fait de diffuser une information basée sur des faits, mais retirée de son contexte d'origine afin d'induire en erreur, de nuire ou de manipuler.

Manipulation de l'information : désigne l'ensemble des actions hostiles visant à diffuser intentionnellement et de manière massive des nouvelles falsifiées, déformées ou décontextualisées.

Mésinformation : diffusion inconsciente ou involontaire d'informations erronées sans intention de nuire. La **désinformation** consiste, elle, en la diffusion délibérée d'informations fausses, incorrectes ou trompeuses dans l'intention de nuire.

Mode opératoire informationnel (MOI) : défini par VIGINUM comme un ensemble de comportements, d'outils, de tactiques, techniques et procédures (TTP) et de ressources adverses présumés liés au même acteur malveillant ou groupe d'acteurs malveillants.

Opération informationnelle : déclinaison des objectifs de la campagne informationnelle en actions afin de diffuser, *via* des ressources numériques (sites *web*, comptes de réseaux sociaux), un narratif et un contenu spécifiques. Exemple : diffusion coordonnée au moyen du MOI *Storm-1516* d'une fausse vidéo affirmant qu'un candidat souhaite transformer le Centre Pompidou en un lieu d'accueil pour migrants.

Surinformation : situation dans laquelle se trouve une personne recevant un flux d'information dans une quantité supérieure à ce qu'elle peut assimiler. En conséquence, cela peut créer une anxiété vis-à-vis de l'information, mais aussi porter atteinte à son esprit critique puisque la personne n'a pas le temps d'aller vérifier tous les éléments d'une information.

5.2 Des techniques variées

Les acteurs de la menace suivis par VIGINUM ont recours à différentes tactiques, techniques et procédures (TTP) qui sont aujourd'hui bien documentées par le service et citées dans ses rapports publics. En voici quelques-unes :

Astroturfing : technique consistant à augmenter artificiellement la visibilité d'un sujet par l'action coordonnée d'un groupe restreint de comptes qui vont produire un volume important de publications. Cette technique sert à faire croire qu'un sujet est un phénomène de masse. L'*astroturfing* a par exemple été utilisé dans le cadre des élections roumaines de 2024 pour promouvoir le candidat Călin GEORGESCU.

Comptes inauthentiques : de nombreux modes opératoires informationnels documentés par VIGINUM ont recours à la création et à l'animation de comptes inauthentiques sur les plateformes en ligne, qui peuvent être automatisés ou administrés par de vraies personnes. Citons par exemple :

- **les « bots »** : technique consistant en l'utilisation d'avatars sur les réseaux sociaux dont les actions ou la création ont été automatisées par un programme informatique pour simuler le comportement d'un être humain. Un bot peut être capable de faire des publications, de laisser des commentaires, de suivre des comptes, de partager ou d'aimer d'autres publications ;
- **les « trolls »** : ce sont des comptes ou des groupes de comptes derrières lesquels se cachent des personnes réelles qui, par jeu, moquerie, activisme politique ou encore par stratégie, insultent,

offensent ou provoquent la polémique sur un sujet afin de déstabiliser le débat public numérique. À l'opposé des bots, les trolls ne sont pas des comptes automatisés.

Copy pasta : technique consistant à publier sur une ou plusieurs plateformes *web*, un même bloc de texte ou de visuel selon la technique du copier-coller, en y ajoutant des légères modifications (émoticônes, ponctuation, *etc*.) dans le but d'amplifier la visibilité d'un message sans se faire censurer par les plateformes. Par exemple, dans le cadre de ses opérations informationnelles, le *Baku Initiative Group* recoure régulièrement à cette technique pour propager ses contenus sur les réseaux sociaux.

IA générative : technique consistant à utiliser des modèles d'intelligence artificielle (IA) générative, capable de créer des contenus (texte, image, vidéo, musique) à partir d'un prompt donné à la machine, afin de produire des contenus originaux imitant des réalisations humaines. C'est notamment le cas des vidéos de type *deepfake* comme celles créées au moyen du mode opératoire informationnel *Storm-1516*.

Typosquatting : technique consistant à usurper l'identité de sites *web* connus en enregistrant un nom de domaine très proche du nom de domaine officiel (ex : *diplomatie.gouv.fm* au lieu de *diplomatie. gouv.fr*). Cette technique sert à tromper les internautes peu avertis. Le mode opératoire informationnel *RRN/Doppelgänger* a souvent recours à cette technique.

À PROPOS DE VIGINUM

Créé le 13 juillet 2021 et rattaché au SGDSN, le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM) a pour raison d'être la protection du débat public numérique touchant aux intérêts fondamentaux de la Nation.

Ce service technique et opérationnel de l'État a pour mission de détecter et caractériser les campagnes de manipulation de l'information sur les plateformes numériques, impliquant des acteurs étrangers dans le but de nuire à la France et à ses intérêts.

Service de vigilance et protection contre les ingérences numériques étrangères | SGDSN

Crédit photo couverture : Photo de João Marcelo Martins sur Unsplash