RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

VIGINUM

Protéger le débat public numérique en contexte électoral

Guide de sensibilisation à l'attention des équipes de campagne

Sommaire

Qu'est-ce que la menace informationnelle ?

Composante à part entière des menaces dites « hybrides », la menace informationnelle en ligne se traduit par la manifestation d'opérations d'ingérences numériques étrangères, qui ont pour objectifs de porter atteinte au fonctionnement des processus démocratiques, de nuire aux intérêts de l'entité ou la personne ciblée et/ou de promouvoir les revendications d'un acteur hostile.

Les ingérences numériques étrangères constituent une menace particulièrement grave pour le fonctionnement démocratique de nos sociétés. Prenant la forme de campagnes planifiées ou d'actions opportunistes, ces manœuvres visent à créer et/ou amplifier des contenus malveillants, à exploiter des faits et/ou évènements sociétaux ou politiques marquants, pour *in fine* exacerber des divisions sociétales autour de thématiques clivantes.

Une menace ciblant particulièrement les processus électoraux

Les élections, symbole de la démocratie et de ses valeurs intrinsèques, constituent dès lors une cible de choix pour les acteurs étrangers désireux d'en déstabiliser le fonctionnement. Ils cherchent notamment à saper, voire à **rompre le lien de confiance entre les citoyens et les citoyennes et les institutions chargées de les représenter**.

Cette volonté de déstabiliser les scrutins électoraux s'opère principalement en amont et durant les phases de campagne électorale.

Les 15 et 22 mars 2026, les électrices et électeurs français seront appelés aux urnes lors des élections municipales. Cette période électorale nationale offre une surface d'exposition informationnelle majeure aux acteurs étrangers désireux **d'altérer la sincérité des débats, et l'intégrité des opérations électorales**.

Quels sont les risques en période électorale ?

Principalement incarnée par des modes opératoires informationnels[1] (MOI) prépositionnés, la menace d'ingérence numérique étrangère en période électorale a pour effet de déstabiliser le processus démocratique en s'attaquant à sa légitimité et à la crédibilité des institutions chargées de son bon déroulement. Cette finalité malveillante peut être atteinte au travers de plusieurs stratégies :

- **La décrédibilisation de la procédure électorale** : le processus démocratique est présenté comme faussé, insincère, inutile, voire manipulé par les autorités en charge de son organisation ;
- **La polarisation du débat politique autour de thématiques clivantes** : des sujets sensibles, susceptibles d'influencer les décisions des électeurs, sont instrumentalisés ou amplifiés afin de nourrir la polarisation de la société et d'accroître ses divisions (politiques publiques, place des minorités, violences policières, débats religieux, etc.) ;
- **La défiance vis-à-vis des médias d'information** : cette stratégie consiste à délégitimer les médias (privés ou publics) afin de remettre en question l'honnêteté et l'authenticité des informations diffusées, de semer la confusion et de pousser les citoyens et citoyennes à se réorienter vers des sources d'informations alternatives, susceptibles d'être manipulées par des acteurs étrangers ;
- **L'exposition réputationnelle d'un(e) candidat, une candidate ou d'un parti politique** : l'ingérence numérique a pour objectif de nuire à la réputation d'une personne candidate ou d'un parti politique impliqués dans la campagne électorale.

[1] Les termes techniques utilisés dans ce guide sont définis en page 11.

Quels sont les techniques utilisées ?

Les modes opératoires utilisés par les acteurs de la menace informationnelle s'appuient sur des techniques, tactiques et procédures de plus en plus sophistiquées.

L'usurpation d'identité d'une institution, d'un média légitime ou d'une formation politique

Cette pratique consiste à tromper l'internaute en créant des sites *web* usurpant l'identité visuelle d'une organisation connue du grand public (média, service public, parti politique, etc.).

Ce mode opératoire s'appuie sur deux techniques :

- le *typosquatting*, qui consiste à usurper l'identité du site *web* d'une organisation en enregistrant un nom de domaine très proche du nom de domaine officiel (par exemple, enregistrement en .fm au lieu de .fr) ;
- l'usurpation de la charte graphique de l'entité ciblée, pour tromper l'internaute.

> **Exemples** : en France et en Europe, plusieurs médias ont été victimes d'usurpations d'identité lors de campagnes menées au moyen du mode opératoire informationnel pro-russe *Matriochka*.
>
> Cette technique a été également utilisée par le mode opératoire informationnel pro-russe *Storm-1516* lors des élections législatives anticipées françaises de juillet 2024, avec notamment la création d'un faux site internet de la coalisation *Ensemble* du parti Renaissance[2]. Le faux site affirmait que la coalition proposait aux électeurs de recevoir une prime d'une valeur de 100 euros en échange de leur voix.

La création de faux reportages par de faux médias

Cette tactique consiste à créer de faux médias présentés comme des médias légitimes afin de véhiculer de faux articles ou de blanchir de faux témoignages ou reportages.

> **Exemple** : cette technique a été utilisée lors des élections présidentielles américaines de novembre 2024 par le mode opératoire informationnel pro-iranien *Storm-2035*, qui avait créé quatre faux sites de presse produisant des messages visant à polariser le débat public numérique américain[3].

[2] VIGINUM – Analyse du mode opératoire informationnel russe Storm-1516 | urlr.me/NsRmdZ
[3] *Microsoft Threat Intelligence Report - Iran steps into US election 2024 with cyber-enabled influence operations* | urlr.me/dejJwz

L'instrumentalisation de la procédure électorale

Cette tactique consiste à manipuler l'information concernant le déroulé de la procédure électorale (fausses informations sur les dates du scrutin par exemple), ou à sous-entendre que la procédure serait faussée ou frauduleuse, en vue de réduire la participation du corps électoral le jour du vote.

> **Exemple** : ce mode opératoire a été utilisé par des acteurs pro-russes lors des élections générales espagnoles de 2023, qui avaient relayé de fausses informations telles que la présence de faux bulletins de vote ainsi qu'une fausse alerte terroriste[4].

Le recours à des comptes inauthentiques

Cette technique consiste à utiliser des réseaux de comptes aux caractéristiques inauthentiques (des *bots* ou des *trolls*), afin d'amplifier de manière artificielle la diffusion de contenus et narratifs.

Ces comptes peuvent avoir recours à la technique de l'*astroturfing*, consistant à diffuser de manière coordonnée, parfois massive, des publications dans le but d'atteindre une vaste audience ou de donner l'impression trompeuse qu'un sujet est extrêmement visible sur les réseaux sociaux.

Ils peuvent également avoir recours au *copy-pasta*, une technique consistant à copier-coller un bloc de texte à l'identique ou presque sur une ou plusieurs plateformes *web*, dans le but d'amplifier la visibilité d'un message.

> **Exemple** : des acteurs pro-russes ont utilisé ce mode opératoire lors des élections américaines de mi-mandat en 2022 ; des comptes inauthentiques avaient notamment repartagé massivement des contenus ciblant la politique d'aide à l'Ukraine de Joe Biden et du camp Démocrate[5].

[4] *SEAE - 2nd EEAS Report on Foreign Information Manipulation and Interference Threats*| urlr.me/TQBq5t
[5] *The New York Times – Russia reactivates its trolls and bots ahead of Tuesday's Midterms* | urlr.me/wG7sRZ

La diffusion de contenus politiques via les publicités en ligne

Cette tactique consiste à détourner le système de publicités en ligne et contourner les règles de modération des plateformes, pour diffuser des contenus sponsorisés polarisants de nature politique.

Elle permet de cibler certaines catégories de la population en fonction de différentes caractéristiques (géographie, âge, etc.), mais également d'atteindre des internautes sans qu'ils soient abonné/es au compte émetteur.

> **Exemple** : cette tactique a été employée par le mode opératoire informationnel pro-russe *RRN*, exposé par la France au mois de juin 2023. VIGINUM a ainsi détecté plusieurs milliers de contenus sponsorisés anti-ukrainiens et pro-russes sur les plateformes, ciblant les audiences françaises[6].

L'amplification d'un narratif par le recours dissimulé à des influenceurs

Cette tactique consiste à utiliser des comptes à moyenne ou forte visibilité (cumulant plusieurs centaines de milliers d'abonnés), contre rémunération ou par connivence idéologique, pour toucher une audience plus large. Elle vise à faire publier par des influenceurs des messages d'apparence anodine relatifs à l'élection ; la plupart de ces messages ne sont néanmoins pas identifiés ni identifiables comme faisant l'objet d'un partenariat rémunéré.

> **Exemple** : ce mode opératoire a été employé pendant les élections présidentielles roumaines de 2024 durant lesquelles plus d'une centaine d'influenceurs, cumulant un total de plus de 8 millions d'abonnés et abonnées, ont été recrutés via des plateformes de marketing d'influence afin de de publier, contre rémunération, des contenus suivant un script et certaines instructions, visant ainsi à visibiliser un des candidats[7].

[6] VIGINUM – RRN : une campagne numérique de manipulation de l'information persistante | urlr.me/JRgaC2

[7] VIGINUM – Manipulation d'algorithmes et instrumentalisation d'influenceurs – Enseignements de l'élection présidentielle en Roumanie et risques pour la France| urlr.me/Z4QefG

La création ou l'amplification de *hashtags* (#)

Cette technique repose sur l'utilisation de *hashtags*, dans le but d'accompagner des narratifs trompeurs ou inexacts afin de faciliter leur diffusion ou leur relai par des internautes légitimes.

> **Exemple** : durant les élections roumaines de 2024, la publication massive et coordonnée de vidéos et de commentaires comportant certains *hashtags* et mots-clefs a permis de manipuler l'algorithme de recommandation de *TikTok* pour propulser la visibilité d'un candidat[8].

La décontextualisation d'images, de vidéos et de propos

Cette pratique consiste à extraire une image, une vidéo ou des propos de leur contexte originel, pour les publier en les rattachant de façon trompeuse à un autre évènement, afin de susciter davantage de réactions et d'engagements.

> **Exemples** : cette technique a été utilisée lors des élections législatives anticipées de 2024 en France. Plusieurs vidéos de violences urbaines ont été présentées comme la conséquence directe des résultats du premier et du second tour, alors que celles-ci avaient été tournées avant les élections législatives dans des contextes différents, tels que des manifestations.

Le recours à l'intelligence artificielle

Cette technique consiste à utiliser des outils d'intelligence artificielle afin de générer du contenu « faux crédible » pouvant servir à appuyer des narratifs. L'IA générative permet ainsi de créer des enregistrements audios ou vidéos réalistes, appelés *deep fakes*, à partir de contenus vrais et facilement accessibles.

> **Exemples** : le mode opératoire informationnel russe *Storm-1516* a recouru à cette technique en amont des élections présidentielles américaines de 2024. Dans une vidéo « *deep fake* » relayée sur *X*, un individu se présente comme un ancien élève de Timothy WALTZ, colistier de Kamala HARRIS, et l'accuse d'agression sexuelle. S'il s'agit bien d'un élève du lycée concerné, ses traits ont été usurpés pour générer la vidéo, potentiellement à partir de photos collectées par les opérateurs sur ses comptes de réseaux sociaux, et ce afin de lui attribuer des propos inauthentiques[9].

[8] VIGINUM – Manipulation d'algorithmes et instrumentalisation d'influenceurs – Enseignements de l'élection présidentielle en Roumanie et risques pour la France| urlr.me/Z4QefG

[9] VIGINUM – Analyse du mode opératoire informationnel russe Storm-1516 | urlr.me/NsRmdZ

Comment se protéger ?

Sensibiliser et se connaître

- Sensibiliser les équipes en interne et acculturer collectivement au risque informationnel
- Définir les sujets et événements susceptibles d'être « manipulés » ou instrumentalisés
- Mettre en place une veille dédiée par des personnes formées au risque d'ingérences numériques étrangères dès la période de campagne électorale

Se préparer

- Organiser des exercices de gestion de crise simulant une attaque informationnelle
- Définir une stratégie de communication de crise adaptée, au sein d'un dispositif interne de réponse établi

Réagir

- Vérifier la source d'une information qui circule sur les réseaux sociaux
- Ne pas relayer l'information et ne pas répondre à une fausse information qui toucherait votre organisation
- Signaler les contenus qui vous semblent faux, trompeurs ou inexacts à l'Arcom et en cas de contenu illicite à la plateforme PHAROS du ministère de l'Intérieur
- Signaler toute toute suspicion de fraude ou d'infraction au code électoral à la police nationale (commissariat de police) ou à la gendarmerie nationale (brigade de gendarmerie) www.masecurite.interieur.gouv.fr ;
- Prendre contact avec VIGINUM lorsque la campagne vous semble provenir d'un acteur étranger : viginum_signalement@sgdsn.gouv.fr

Quel est 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 pour missions principales de **détecter et de caractériser les campagnes de manipulation de l'information sur les plateformes numériques, impliquant des acteurs étrangers, qui ont pour but de nuire à la France et à ses intérêts fondamentaux**. Pour ce faire, le service étudie les phénomènes inauthentiques (comptes suspects, contenus malveillants, comportements anormaux ou coordonnés) qui se manifestent sur les plateformes numériques.

Une ingérence numérique étrangère est ainsi définie selon quatre critères :

- **Son contenu** : les allégations ou imputations de faits manifestement inexactes ou trompeuses ;
- **Son comportement** : l'usage de moyens inauthentiques ou coordonnés (*bots*, *trolls*, faux comptes, 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).

En période électorale, VIGINUM est 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**. Au titre de son décret, le service fournit également **toute information utile aux autorités garantes du bon déroulement du scrutin**.

Lexique de la menace informationnelle

Astroturfing : mode opératoire consistant à conférer de la visibilité à un sujet en faisant croire qu'il est un phénomène de masse alors même qu'il émane de la coordination de quelques comptes produisant un volume important de publications sur un même sujet.

Bot : programme informatique automatisé pour simuler le comportement humain sur les réseaux sociaux. Un *bot* est capable de faire des publications, de laisser des commentaires, de partager ou d'aimer d'autres publications.

Copy-pasta : bloc de texte ou de visuel copié-collé à l'identique ou presque, sur une ou plusieurs plateformes *web*, dans le but d'amplifier la visibilité d'un message.

Deepfake : trucage audio ou vidéo à partir d'éléments existants, utilisant l'intelligence artificielle pour changer le visage d'une personne dans une vidéo ou reproduire sa voix.

Hashtag (#) : mot-clé cliquable, précédé du signe dièse (#), permettant de faire du référencement sur les sites de microblogage.

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.

Manipulation de l'information : ensemble des actions hostiles visant à diffuser intentionnellement et de manière massive des nouvelles falsifiées, déformées (désinformation) ou encore associées à de vraies informations pour les rendre crédibles, sorties de leur contexte ou partielles (malinformation).

Mode opératoire informationnel : ensemble de comportements, d'outils, de tactiques, techniques et procédures et de ressources adverses mis en œuvre par un acteur ou un groupe d'acteurs malveillants dans le cadre d'une ou de plusieurs opérations informationnelles numériques.

Troll : comptes ou groupes de comptes qui, par jeu, moquerie ou activisme politique, perturbent l'espace numérique en cherchant à déstabiliser les débats publics.

Typosquatting : technique qui consiste à enregistrer des noms de domaines avec des URL délibérément mal orthographiés de sites *web* connus pour tromper des internautes peu avertis.

Secrétariat général de la défense et de la sécurité nationale

Conception :
VIGINUM
Décembre 2025

viginum_signalement@sgdsn.gouv.fr

Crédits iconographie :
couverture : juicy_fish - Flaticon ; Freepix
p.9 : Flaticon : Freepik ; Vector Market ;