RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

VIGINUM

# **Protéger le débat public numérique en contexte électoral :** guide de sensibilisation à l'attention des équipes de campagne

Mars 2024

# 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 de manœuvres ou de campagnes numériques de manipulation de l'information, avec pour objectifs de porter atteinte au fonctionnement des processus démocratiques, nuire aux intérêts de l'entité ciblée et/ou promouvoir les revendications d'un acteur.

Prenant la forme d'opérations planifiées ou d'actions opportunistes, ces manœuvres cherchent à diffuser de fausses informations ou à amplifier des contenus malveillants déjà présents dans le débat public.

S'appuyant sur un contexte géopolitique fortement dégradé et caractérisé par la résurgence du rapport de force dans les relations entre puissances, les campagnes numériques de manipulation de l'information sont devenues un véritable instrument de déstabilisation des démocraties.

En 2024, les élections européennes concerneront plus de 400 millions d'électeurs dans les 27 Etats membres. Elles offrent ainsi une surface d'exposition informationnelle majeure aux acteurs étrangers malveillants désireux d'altérer la sincérité des débats numériques, et *in fine* le vote des citoyens européens.

# Les risques en période électorale

En période électorale, la menace informationnelle est susceptible de déployer les stratégies suivantes :

### La décrédibilisation de la procédure électorale

Le processus démocratique est présenté d'emblée comme faussé, insincère, inutile, voire manipulé par les autorités en charge de son organisation.

### La polarisation du débat politique autour de thématiques clivantes

Les décisions et les actions des autorités politiques sont systématiquement remises en question afin de nourrir la polarisation de la société autour de thématiques clivantes (politiques publiques, place des minorités, violences policières, débats religieux, etc.).

### La défiance vis-à-vis des médias traditionnels

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 à se réorienter vers des sources d'informations alternatives, susceptibles d'être manipulées.

### L'exposition réputationnelle d'un(e) candidat(e) ou d'un parti politique

L'ingérence numérique a pour objectif de modifier la perception d'un candidat ou de son image, en fonction des circonstances.

# Quelques modes opératoires utilisés

## L'amplification de narratifs et/ou de sentiments négatifs via des réseaux de bots et de trolls

Ce mode opératoire consiste à amplifier des narratifs sur un sujet clivant et à modeler de manière sélective des faits autour de ce sujet, au moyen d'un flux constant de publications sur un seul et même axe sémantique.

*Mode opératoire utilisé lors des élections américaines de mi-mandat en 2022.*

## L'usurpation d'identité d'un média légitime

Ce mode opératoire consiste à tromper l'internaute en usurpant l'identité d'un média légitime (création d'un faux site) pour y diffuser du contenu inexact.

*Plusieurs médias français et européens ont été victimes de ce mode opératoire lors de la campagne « RRN ».*

## L'instrumentalisation de la procédure électorale

Ce mode opératoire consiste à manipuler l'information concernant le déroulé de la procédure électorale (fausses informations sur les dates du scrutin par exemple), en vue de réduire la participation des citoyens le jour du vote.

*Mode opératoire utilisé lors des élections générales espagnoles de 2023.*

## La diffusion de publicités politiques en ligne

Ce mode opératoire consiste à détourner le système de publicités en ligne, sur les plateformes, pour diffuser des contenus polarisants de nature politique. Cette diffusion permet de cibler certaines catégories de citoyens en fonction de différentes caractéristiques (géographiques, âge, etc.), mais également d'atteindre des utilisateurs sans qu'ils soient abonnés au compte émetteur.

*Mode opératoire employé dans le cadre de la campagne RRN, exposée 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.*

## L'*astroturfing*

Ce mode opératoire vise à créer ou amplifier un sujet polémique, généralement autour d'un ou plusieurs hashtags, dont les acteurs vont chercher à en augmenter la visibilité. Le recours à la création et au partage massif d'images, permet une meilleure diffusion des narratifs.

### La fuite délibérée de données ou doxxing

Ce mode opératoire consiste à obtenir, à travers différents procédés, les informations sensibles d'un candidat, ou d'une équipe de campagne, pour les publier sur Internet afin de dénigrer leur image.

*Mode opératoire mis en œuvre au cours de l'élection présidentielle française de 2017 pour diffuser de fausses informations sur le candidat Emmanuel Macron*

### La publication de contenus fabriqués sur des médias et des comptes de réseaux sociaux

Ce mode opératoire consiste à usurper sur les réseaux sociaux, l'identité d'un candidat ou d'une candidate afin de véhiculer de fausses informations pouvant lui nuire. Il implique également la possibilité de prendre le contrôle de médias, ou de comptes authentiques sur les réseaux sociaux, pour y publier des contenus faux ou trompeurs.

*Cette tactique a notamment été utilisé par le mode opératoire Ghostwriter exposé par l'Union européenne en 2021, en amont des élections fédérales allemandes. Après avoir compromis le système d'information d'un média légitime, les attaquants ont publié des faux articles écrits par des auteurs fictifs, et les ont diffusés via de faux mails institutionnels. Si la nature de la compromission est d'origine cyber, ses effets les plus notables peuvent en revanche être informationnels. .*

### L'incitation à conduire des actions dans le champ physique

Ce mode opératoire peut se traduire en ligne par des appels à manifester ou à dégrader des bureaux de votes, ou des locaux de partis politiques. Les effets produits dans la vie réelle peuvent, par la suite, être instrumentalisés dans le champ informationnel. .

*Mode opératoire utilisé lors de l'élection présidentielle américaine de 2016 : de fausses pages Facebook administrées par un acteur étranger ont organisé des manifestations pro-TRUMP dans plusieurs villes des États-Unis, via la fonction « évènements » proposée par la plateforme.*

### La création de vidéo de type deep fake

Ce mode opératoire consiste à créer un enregistrement vidéo ou audio réalisé ou modifié grâce à l'intelligence artificielle. S'appuyant sur la technologie du deep learning, ce procédé permet de générer du faux crédible, à partir de contenus vrais et facilement accessibles.

# 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.

## Se préparer :

- organiser des exercices de gestion de crise simulant une attaque informationnelle ;
- définir une stratégie de communication de crise adaptée.

## 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[1] et en cas de contenu illicite à la plateforme PHAROS[2] du ministère de l'Intérieur;
- prendre contact avec VIGINUM lorsque la campagne vous semble provenir d'un acteur étranger : **viginum_signalement@sgdsn.gouv.fr**

[1] www.arcom.fr/alertez-nous/signaler-un-contenu-sur-internet
[2] www.internet-signalement.gouv.fr/PharosS1/

# Qu'est-ce que VIGINUM ?

Créé le 13 juillet 2021 et rattaché au Secrétariat général de la défense et de la sécurité nationale, VIGINUM est le service de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères. Il 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.

Les élections étant un élément fondamental du processus démocratique en France, 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 pendant les périodes électorales. VIGINUM fournit ainsi toute information utile aux autorités garantes du bon déroulement du scrutin.

Si vous pensez que votre organisation est victime d'une campagne numérique de manipulation de l'information relevant de l'ingérence numérique étrangère, contactez VIGINUM : **viginum_signalement@sgdsn.gouv.fr**

VIGINUM

**Secrétariat général de la défense et de la sécurité nationale**

**viginum_signalement@sgdsn.gouv.fr**