PREMIER MINISTRE

Liberté
Égalité
Fraternité

VIGINUM

01 DÉCOUVRIR VIGINUM

VIGINUM

VIGINUM est le service de vigilance et de protection contre les ingérences numériques étrangères (INE).

VIGINUM a été créé par le décret n° 2021-922[1] du 13 juillet 2021, pour renforcer le dispositif français de lutte contre les ingérences numériques étrangères.

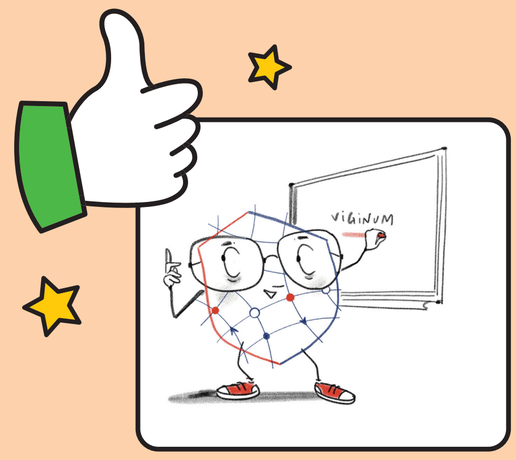
Il est rattaché au secrétariat général de la défense et de la sécurité nationale (SGDSN).

Son rôle : coordonner, en lien avec les ministères, les travaux visant à assurer la sécurité et l'intégrité des intérêts de la France.

SES MISSIONS :

- Détecter, caractériser et documenter les INE (manœuvres informationnelles numériques orchestrées par des acteurs étrangers).
- Contribuer à la recherche et au développement d'outils, d'algorithmes et de modèles susceptibles d'être mobilisés dans l'exercice de détection, de caractérisation et de documentation des INE.
- Sensibiliser, former et accompagner la société civile.

VIGINUM



SA MÉTHODE DE TRAVAIL : l'exploitation des sources ouvertes sur internet

Le renseignement de sources ouvertes – ou renseignement d'origine sources ouvertes (ROSO), «*Open Source Intelligence*» (OSINT) en anglais – est une technique de renseignement permettant de collecter des informations librement accessibles par tous sur internet.

VIGINUM utilise uniquement des techniques d'OSINT pour détecter et caractériser des ingérences numériques étrangères.

QUIZ

Parmi ces trois propositions, laquelle constitue une technique de recherche en sources ouvertes ?

A. Mettre sur écoute le téléphone d'un individu pour connaître le contenu de ses appels

B. Menacer un individu dans une ruelle sombre pour lui soutirer des informations

C. Recueillir des renseignements à partir d'informations librement accessibles sur internet

Réponse : recueillir des renseignements à partir d'informations librement accessibles sur internet

1. Ce décret a été modifié par le décret n° 2026-70 du 11 février 2026 relatif aux missions et moyens du service de vigilance et de protection contre les ingérences numériques étrangères.

PREMIER MINISTRE

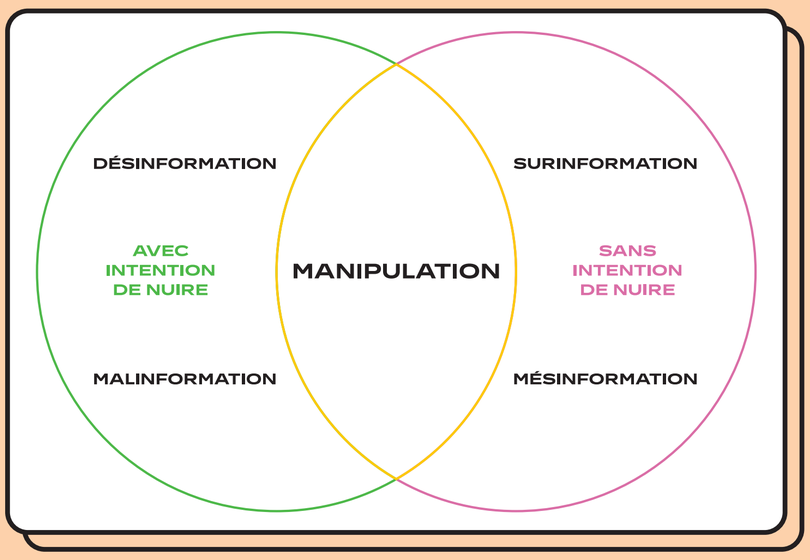
Liberté
Égalité
Fraternité

VIGINUM

02

GLOSSAIRE DE LA LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION (LMI)







La **manipulation de l'information** désigne un ensemble d'actions destinées à tromper les individus, en diffusant en grand nombre des informations inventées ou des faits réels déformés ou sortis de leur contexte.

- La **désinformation** est le fait de partager volontairement des informations fausses pour tromper les personnes.

- La **malinformation** désigne une situation où un individu diffuse une information vraie, mais pour nuire à une personne, un groupe ou un pays.

- La **mésinformation** est une situation où une information incorrecte est transmise, mais sans intention de nuire. La personne qui la partage pense souvent elle-même que l'information est vraie.

- La **surinformation** est une situation où une personne reçoit tellement d'informations qu'elle ne peut ni tout comprendre ni tout vérifier. Cela peut créer du stress, rendre la compréhension difficile et empêcher de développer un esprit critique.

Un **mode opératoire informationnel** (MOI) est défini par VIGINUM comme un ensemble de comportements, d'outils ainsi que de tactiques, techniques et procédures (on parle de « TTP ») et de ressources adverses mises en œuvre par un acteur ou un groupe d'acteurs malveillants dans le cadre d'une ou de plusieurs opérations informationnelles numériques.

QUIZ

Un individu repartage sans le savoir sur les réseaux sociaux une affirmation erronée au sujet d'émeutes en marge d'une compétition sportive. **À quel type de manipulation de l'information renvoie cette manœuvre ?**

A Désinformation

B Mésinformation

C Malinformation

D Surinformation

Réponse : mésinformation

PREMIER MINISTRE

Liberté
Égalité
Fraternité

VIGINUM

03

FOCUS SUR LES INGÉRENCES NUMÉRIQUES ÉTRANGÈRES

QUELS SONT LES QUATRE CRITÈRES QUI DÉFINISSENT UNE INGÉRENCE NUMÉRIQUE ÉTRANGÈRE ?

Découvrez-les à l'aide d'exemples tirés du rapport de VIGINUM décrivant le mode opératoire informationnel *Storm-1516* :



01 Le mode opératoire informationnel (MOI) russe *Storm-1516* a ciblé les élections européennes de juin 2024, les élections législatives anticipées de juillet 2024 et les élections municipales de 2026. Ces manœuvres avaient pour objectif de dénigrer des candidats ou de soutenir d'autres partis ou candidats favorables aux intérêts russes.

02 Pour mettre en œuvre leurs campagnes informationnelles, les acteurs du MOI *Storm-1516* ont eu recours à des outils permettant de générer des voix ou des images de manière artificielle. Ces outils ont notamment permis d'usurper l'identité de personnalités publiques.

03 Les faux récits diffusés par le mode opératoire informationnel *Storm-1516* ont été amplifiés par un réseau d'acteurs russes et par d'autres modes opératoires informationnels (MOI) qui ont agi de manière coordonnée afin de rendre les récits diffusés les plus crédibles possible.

04 Les investigations de VIGINUM, qui s'appuient sur des éléments révélés en source ouverte, confirment l'implication d'individus et d'organisations proches du gouvernement russe.

Une ingérence numérique étrangère est définie par quatre critères :

01

Une atteinte potentielle aux **intérêts fondamentaux de la Nation** définis par le Code pénal (fonctionnement des institutions, intérêts économiques, politique étrangère, etc.).

02

Un **contenu** manifestement inexact ou trompeur.

03

Une **diffusion** ou une volonté de diffusion artificielle ou automatisée, massive et délibérée.

04

L'implication, directe ou indirecte, d'un **acteur étranger** (étatique, paraétatique ou non étatique).

Si ces quatre critères ne sont pas réunis, une campagne de manipulation de l'information ne peut pas être qualifiée d'ingérence numérique étrangère.

QUIZ

Lors des élections municipales en France, un candidat à la mairie entreprend une vaste campagne de manipulation de l'information à l'encontre de son adversaire. **S'agit-il d'une ingérence numérique étrangère ?**

A. OUI B. NON

Réponse : non

PREMIER MINISTRE

Liberté
Égalité
Fraternité

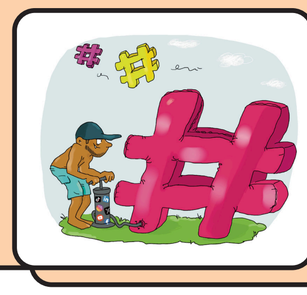
VIGINUM

04 LES MAUX DE L'INFO

Les acteurs de la menace suivis par VIGINUM ont recours à différentes tactiques, techniques et procédures citées dans ses rapports publics. En voici quelques-unes :

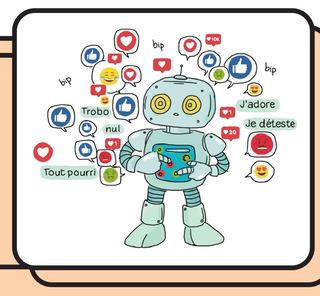


***Typosquatting* :** technique consistant à usurper l'identité de sites web connus en enregistrant un nom de domaine très proche du nom de domaine officiel (ex. pronote.fm au lieu de pronote.fr). Cette technique sert à tromper les internautes.

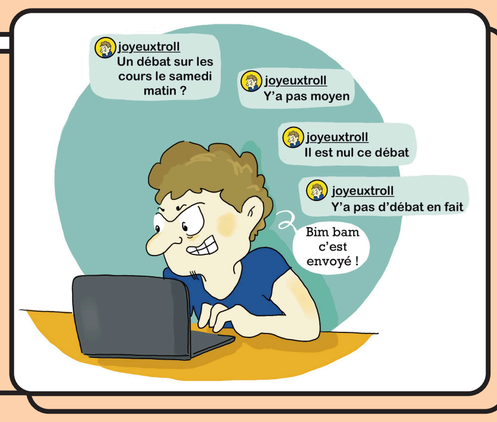


***Astroturfing* :** technique consistant à augmenter artificiellement la visibilité d'un sujet par l'action coordonnée d'un groupe restreint de comptes qui vont produire un volume important de publications. Cette technique sert à faire croire qu'un sujet est un phénomène de masse. L'*astroturfing* a,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

Comptes inauthentiques : de nombreux modes opératoires informationnels 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 :



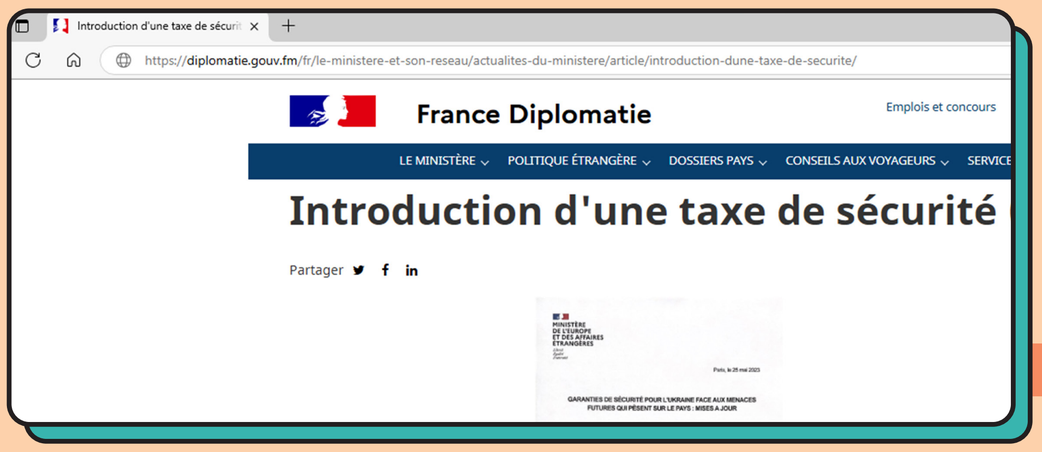
- **Les *bots*** : technique consistant en l'utilisation d'avatars sur les réseaux sociaux dont la création ou les actions ont été automatisées par un programme informatique pour simuler le comportement d'un être humain. Un *bot* peut être capable de faire des publications, de laisser des commentaires, de suivre des comptes, de partager ou d'aimer d'autres publications.



- **Les *trolls* :** ce sont des comptes ou des groupes de comptes derrière 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.

EXERCICE

Sauriez-vous rattacher cet exemple à une définition ?



Réponse : il s'agit de *typosquatting*. En voici un exemple : le site officiel « France Diplomatie » a été usurpé, comme l'indique le nom de domaine diplomatie.gouv.fm, et non diplomatie.gouv.fr. Cette technique a été documentée dans le rapport « RNN : une campagne numérique de manipulation de l'information complexe et persistante ». ..... →

©Véropée

PREMIER MINISTRE

Liberté
Égalité
Fraternité

VIGINUM

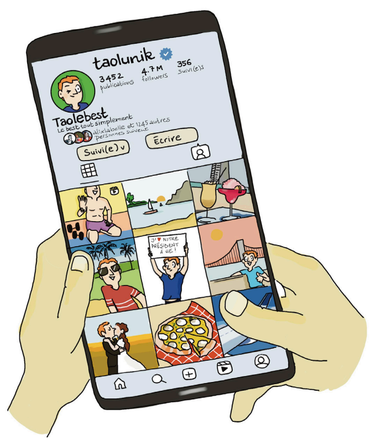
05

LES MAUX DE L'INFO, LA SUITE

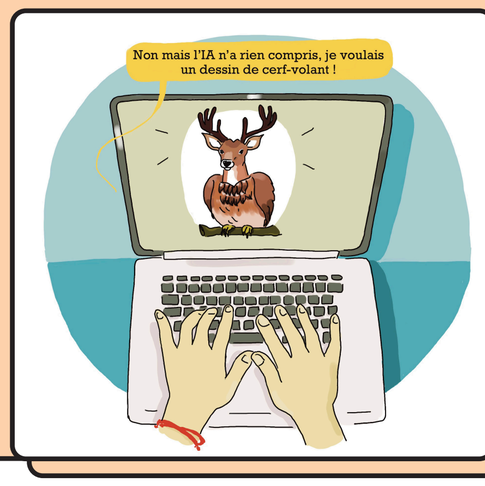
Les acteurs de la menace suivis par VIGINUM ont recours à différentes tactiques, techniques et procédures citées dans ses rapports publics. En voici quelques-unes :



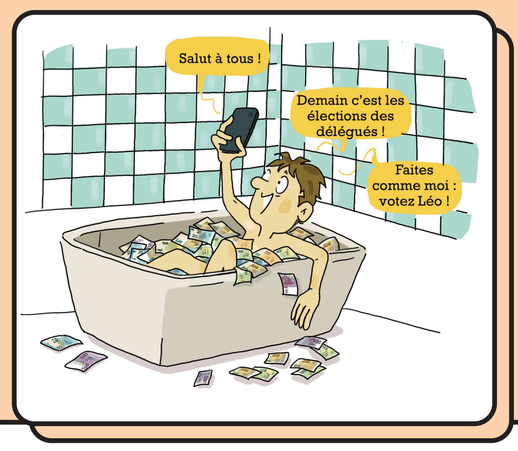
***Copy pasta* :** technique consistant à publier, sur une ou plusieurs plateformes web, un même bloc de texte ou de visuel par simple copier-coller, en y ajoutant de légères modifications (émoticônes, ponctuation, etc.) dans le but d'amplifier la visibilité d'un message sans se faire censurer par les plateformes.



Spammouflage : technique consistant en la diffusion de messages de nature politique dissimulés au milieu de publications aux sujets plus anodins (musique, cuisine, sport, *lifestyle*, etc.).



IA générative : technique consistant à utiliser des modèles d'intelligence artificielle (IA) générative capables 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.



Recours à des influenceurs : technique consistant à utiliser des comptes disposant d'une forte audience, en l'espèce des comptes cumulant plusieurs milliers d'abonnés et/ou entretenant une relation avec leur communauté, pour amplifier la diffusion d'un contenu et ainsi lui permettre de toucher une audience plus large.

EXERCICE

Sauriez-vous rattacher cet exemple à une définition ?



©Véropée

Réponse : il s'agit de *copy pasta*. En voici, ci-dessus, un exemple : la phrase est copiée-collée dans plusieurs publications postées sur *X*; seules de petites modifications apparaissent.

PREMIER MINISTRE

Liberté
Égalité
Fraternité

VIGINUM

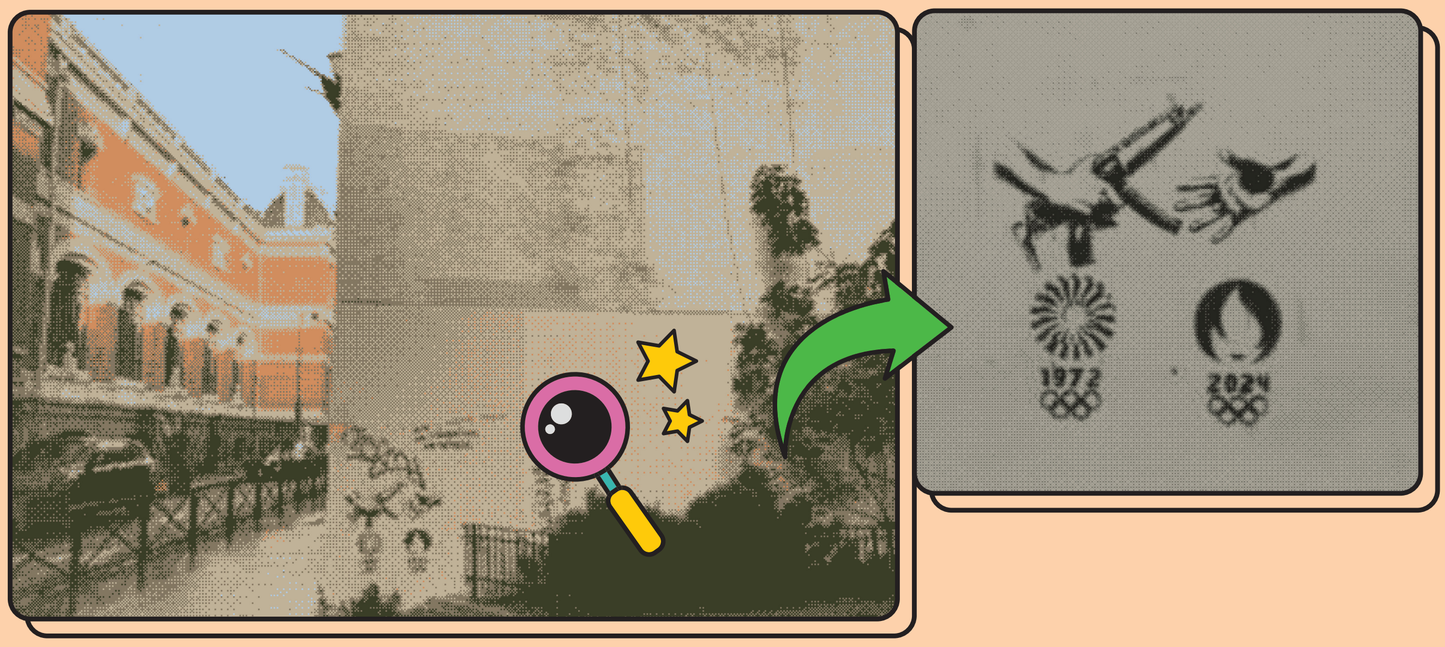
06

L'IMPACT DES INGÉRENCES NUMÉRIQUES ÉTRANGÈRES

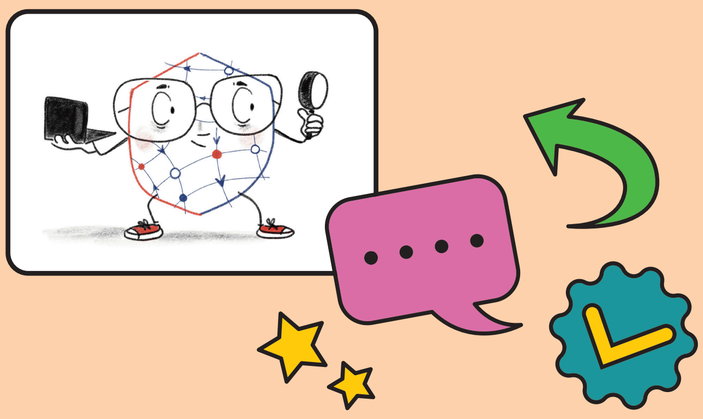
Les ingérences numériques étrangères peuvent avoir des conséquences dans le débat public numérique, mais également dans le champ physique. Elles peuvent, par exemple :

- altérer l'information diffusée aux citoyens ;
- délégitimer les institutions publiques ;
- décrédibiliser l'image de la France ;
- porter atteinte aux activités économiques de la France ;
- polariser le débat public ;
- troubler l'ordre public.

Pendant les Jeux olympiques et paralympiques de Paris 2024, de nombreux acteurs ont tenté de porter atteinte à la crédibilité de la France et à sa capacité à accueillir les Jeux. Les acteurs malveillants ont tenté, par exemple, d'amplifier la visibilité en ligne de manœuvres orchestrées sur le champ physique. En novembre 2023, VIGINUM a ainsi repéré, sur les plateformes *Telegram*, *VK*, *Facebook* et *X*, plusieurs images de graffitis représentant deux mains se transmettant une arme, placées au-dessus des logos des Jeux olympiques de Munich 1972 et de Paris 2024. L'authenticité de ces images n'a pas pu être établie ; pour autant, leur diffusion a été amplifiée par plusieurs comptes présentant des comportements inauthentiques.



Graffitis prétendument localisés au 13, rue Buffon, Paris 5e, à 750 mètres de la Grande Mosquée de Paris.



QUIZ

Une manœuvre informationnelle en ligne n'a jamais d'impact sur le champ physique.

A. VRAI B. FAUX

Réponse : faux

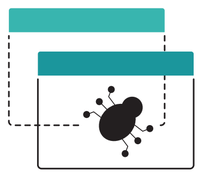
PREMIER MINISTRE

Liberté
Égalité
Fraternité

VIGINUM

07

DES CONSEILS POUR RENFORCER SON ESPRIT CRITIQUE



ADOPTEZ UNE POSTURE CRITIQUE

Prenez du recul sur l'information que vous voyez, méfiez-vous des titres trop accrocheurs ou qui font appel aux émotions.



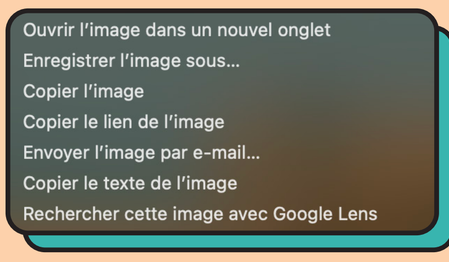
ANALYSEZ L'AUTHENTICITÉ DE LA SOURCE

Des éléments peuvent vous donner des indices pour constater que c'est un faux compte :

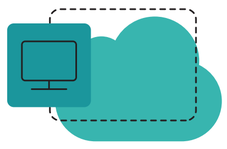
- une date de création très récente;
- un rapport abonnés/abonnements inégal (1 abonné pour 138 abonnements, par exemple);
- un horaire de publication similaire pour chaque publication (chaque publication est postée à 18 h 48, par exemple);
- une photo de profil qui semble générée par intelligence artificielle, etc.

ASTUCE

Comment tester une image en ligne en *reverse image* pour vérifier son authenticité ? Cliquez droit et « Rechercher avec Google Lens ».



Et vérifiez si l'image est utilisée dans un autre contexte.



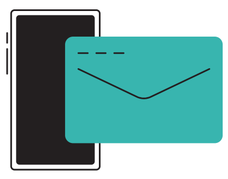
VÉRIFIEZ LES IMAGES

Une recherche inversée d'images et de vidéos peut aider à vérifier si le contenu a déjà été utilisé dans un contexte différent.



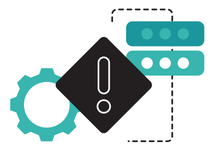
ASSUREZ-VOUS DU CONTENU DE LA SOURCE

Vérifiez les faits et les chiffres qui sont donnés; regardez la date et le contexte de publication de l'article pour en savoir plus sur ce que c'est, d'où ça vient.



RÉFLÉCHISSEZ AVANT DE REPARTAGER

Face à la manipulation d'une information, on peut avoir un rôle à jouer. Il est important de ne pas repartager des contenus douteux; cela permet de casser la chaîne de diffusion provenant d'une source inauthentique.



SIGNALEZ DES CONTENUS ILLICITES

Vous pouvez aussi signaler des contenus, soit directement auprès des plateformes concernées, soit auprès de Pharos, le portail officiel de signalement des contenus illicites sur internet. Si vous vous trouvez face à une information qui vous semble fausse, n'hésitez pas à prévenir un adulte qui pourra agir pour la signaler.

PREMIER MINISTRE

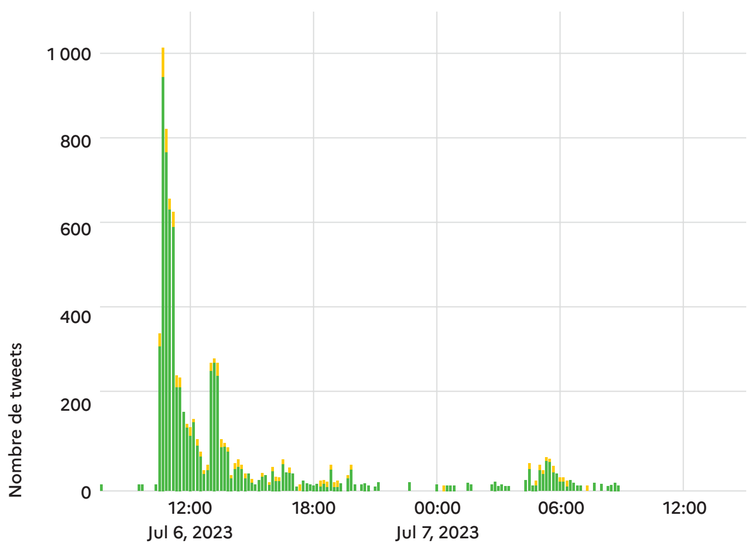
Liberté
Égalité
Fraternité

VIGINUM

08

À LA DÉCOUVERTE DU RAPPORT BIG





Nombre de publications partageant les hashtags #NonAlignedMovement #France #Colonialism par tranche de dix minutes. En vert, les publications originales ; en jaune, les republications.

DÉCEMBRE 2024, LE *BAKU INITIATIVE GROUP* (BIG)

Le rapport « *UN-notorious BIG* : une campagne numérique de manipulation de l'information ciblant les DROM-COM et la Corse » a été publié en décembre 2024.

Depuis le mois de juillet 2023, VIGINUM suit l'activité numérique d'une organisation en lien avec l'État azerbaïdjanais nommée *Baku Initiative Group* (BIG), ainsi que celle d'un cluster de comptes *X* qui lui est associé. Les acteurs de ce mode opératoire informationnel cherchent à remettre en cause l'intégrité territoriale de la France dans ses territoires ultramarins. En diffusant des contenus dont la ligne éditoriale est hostile à la France, ils instrumentalisent de manière opportuniste les mouvements indépendantistes, notamment lors des périodes de crise, comme en Nouvelle-Calédonie ou en Martinique au cours de l'année 2024.

Le BIG a développé son activité par une action en deux temps :

- premièrement, un réseau de comptes inauthentiques actif sur X amplifie artificiellement la visibilité des conférences et déclarations publiques du BIG ;
- dans un second temps, la posture du BIG a évolué vers une attitude plus institutionnelle, avec la promotion d'événements publics, la signature de mémorandums avec des partis indépendantistes des DROM-COM, la publication de podcasts ou encore de vidéos générées par IA tout en renforçant ses liens avec les mouvements panafricanistes.

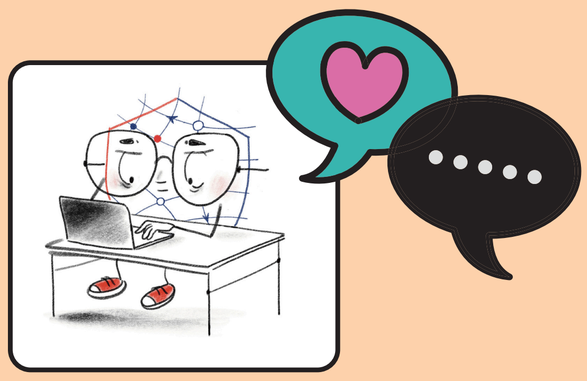
QUIZ

Qu'est-ce que le BIG ?

A. Un service étatique azerbaïdjanais

B. Une organisation liée à l'État azerbaïdjanais

C. Un burger



Réponse : une organisation liée à l'État azerbaïdjanais

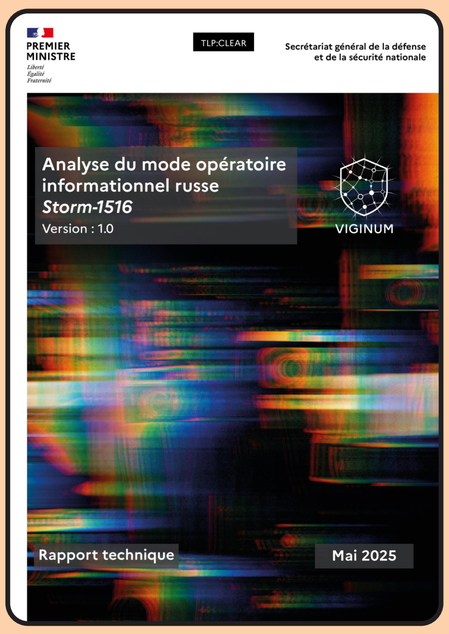
PREMIER MINISTRE

Liberté
Égalité
Fraternité

VIGINUM

04

À LA DÉCOUVERTE DU RAPPORT *STORM-1516*



En mai 2025, après des mois d'enquête, VIGINUM a publié un rapport sur un mode opératoire informationnel russe appelé *Storm-1516*. S'appuyant sur une grande variété de contenus, celui-ci diffuse en ligne de nombreuses informations manipulées.

Le mode opératoire *Storm-1516* a plusieurs cibles et en vise tout particulièrement trois :

- les intérêts ukrainiens. En diffusant largement des informations manipulées, *Storm-1516* vise avant tout à décrédibiliser l'Ukraine auprès des audiences occidentales, notamment pour saper le soutien européen au pays ;
- les intérêts occidentaux. *Storm-1516* cherche aussi à décrédibiliser des dirigeants ou des proches de personnalités politiques européennes ou américaines ;
- les processus électoraux. *Storm-1516* a ciblé les élections européennes de juin 2024, les élections législatives anticipées françaises de juillet 2024, l'élection présidentielle américaine de novembre 2024 et les élections fédérales allemandes de février 2025.

Si l'impact réel sur le débat public numérique est difficile à estimer, une grande partie des contenus diffusés a atteint une visibilité importante en ligne. Ils ont parfois été repartagés, de manière inconsciente ou opportuniste, par des personnalités et des représentants politiques de premier plan, notamment en Europe et en France.

Le mode opératoire *Storm-1516* est toujours actif en 2026. VIGINUM continue de suivre avec attention son activité.

Les différentes opérations informationnelles de *Storm-1516* s'appuient sur une large gamme de contenus, dans de multiples langues :

- des montages photo et vidéo ;



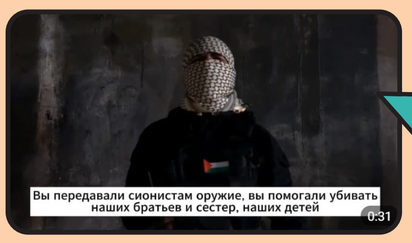
Capture d'écran d'une fausse facture diffusée par *Storm-1516*

- des vidéos et des audios probablement générés par IA afin d'usurper l'identité de personnalités publiques et d'internautes ;



Capture d'écran d'un probable *deepfake* attribué à *Storm-1516*.

- des vidéos impliquant des comédiens amateurs.



Capture d'écran de la vidéo de prétendus membres du Hamas menaçant les Jeux olympiques de Paris 2024.

QUIZ

Le MOI *Storm-1516* a eu recours à différentes techniques, tactiques et procédures. Quelle technique est utilisée ici ?

A. Astroturfing
B. Copy pasta
C. Recrutement de comédiens
D. Typosquatting

Réponse : recrutement de comédiens

PREMIER MINISTRE

Liberté
Égalité
Fraternité

VIGINUM

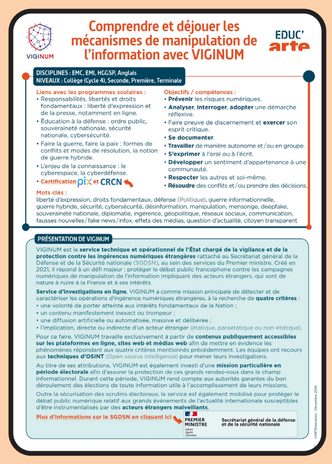
10

LES RESSOURCES DE SENSIBILISATION

VOS IDÉES POUR SENSIBILISER

Pour en savoir plus sur les ingérences numériques étrangères, voici quelques ressources de sensibilisation :

La fiche pédagogique Educ'Arte



Le jeu de plateau « Le Bouclier contre les ingérences numériques étrangères »



Le podcast « Le débrief de Clara et Raphaël »



Le module de formation « Désinformation et ingérences numériques étrangères », à destination des enseignants



Les kits de sensibilisation adultes et enfants



