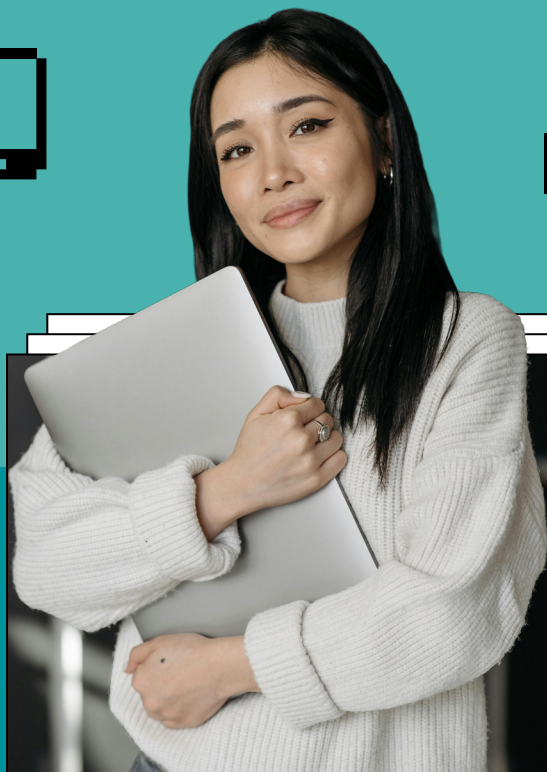


# EN MISSION AVEC VIGINUM

Protéger le débat public  
contre les ingérences numériques étrangères



# SOMMAIRE

DÉFINITIONS ..... 04

TECHNIQUES, TACTIQUES  
ET PROCÉDURES ..... 06

CONSEILS DE  
SENSIBILISATION ..... 08

MISSION

TESTER LE « REVERSE IMAGE »... 10

MISSION

TESTER SES CONNAISSANCES  
ENTRE ADULTES ET JEUNES ..... 12

RAPPORTS  
À LA DÉCOUVERTE  
DU RAPPORT « STORM-1516 » .... 14

RAPPORTS  
À LA DÉCOUVERTE DU  
RAPPORT « MATRIOCHKA » ..... 18

RAPPORTS  
À LA DÉCOUVERTE  
DU RAPPORT SUR LES  
ÉLECTIONS EN ROUMANIE ..... 22

NOS CONTENUS  
DE SENSIBILISATION ..... 24

CORRECTION DES JEUX ..... 26

# PRÉSENTATION DE VIGINUM

**VIGINUM** est le service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères, rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN). Créé en 2021, il répond à un défi majeur : protéger le débat public francophone contre les campagnes numériques de manipulation de l'information menées par des acteurs étrangers, qui sont de nature à nuire à la France et à ses intérêts.

Service d'investigations en ligne, VIGINUM a pour mission principale de détecter et de caractériser les opérations d'ingérences numériques étrangères. Une ingérence numérique étrangère est **un phénomène inauthentique affectant le débat public** numérique qui combine les quatre critères suivants :

- une atteinte potentielle **aux intérêts fondamentaux de la Nation**, notamment définis par le Code pénal (fonctionnement des institutions, intérêts économiques, politique étrangère, etc.);
- un **contenu** manifestement inexact ou trompeur;
- une **diffusion**, ou une volonté de diffusion, artificielle ou automatisée, massive et délibérée;
- l'**implication**, directe ou indirecte, d'un **acteur étranger** (étatique, paraétatique ou non étatique).

Pour détecter et caractériser des campagnes informationnelles venues de l'étranger, VIGINUM travaille uniquement à partir de méthodes d'**OSINT** : **l'Open Source Intelligence ou le Renseignement d'origine sources ouvertes est une méthode de renseignement utilisant des sources d'information publiques.**

Ce livret présente le service de vigilance et de protection contre les ingérences étrangères, ses missions, ainsi que le fonctionnement d'une campagne de manipulation de l'information orchestrée par des acteurs étrangers.

Il s'inscrit dans une démarche globale de sensibilisation du grand public et complète le livret destiné au jeune public, afin d'offrir, ensemble, une compréhension cohérente et adaptée des enjeux liés à la lutte contre les ingérences numériques étrangères et les manipulations de l'information. Un exercice à faire en famille et/ou en classe est prévu à la fin du livret.

Le livret destiné au jeune public vient vulgariser les informations présentées ici, et apporte des exercices complémentaires sous forme de missions.

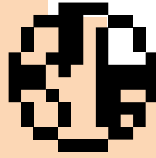


# DÉFINITIONS

Quelques éléments de définition pour commencer.

Quand on parle de manipulations de l'information, différents termes peuvent être employés. Afin de bien appréhender le sujet, il est nécessaire de distinguer les différents phénomènes auxquels ils font référence.





**La désinformation** consiste en la diffusion délibérée d'informations fausses, incorrectes ou trompeuses dans l'intention de nuire.

**La malinformation** est une information qui se fonde sur la réalité, mais qui est utilisée pour porter préjudice à une personne, une organisation ou un pays.

**La mésinformation** correspond à la diffusion inconsciente ou involontaire d'informations erronées, sans intention de nuire.

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

**La manipulation de l'information**, dont font partie les ingérences numériques étrangères, désigne l'ensemble des actions hostiles visant à diffuser intentionnellement et de manière massive des nouvelles falsifiées, déformées, ou encore associées à de vraies informations pour les rendre crédibles, mais sorties de leur contexte.

**Un mode opératoire informationnel (MOI)** est défini par VIGINUM comme un ensemble de comportements, d'outils, mais aussi de tactiques, techniques et procédures (on parle de « TTP »), 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.

**Une opération informationnelle** décrit l'utilisation ponctuelle, par un mode opératoire informationnel, de certaines ressources informationnelles (sites web, comptes de réseaux sociaux) et de TTP pour répondre à des objectifs tactiques préalablement fixés.

**Une campagne informationnelle** désigne quant à elle un ensemble d'opérations informationnelles mises en œuvre par un mode opératoire pour répondre à des objectifs stratégiques.

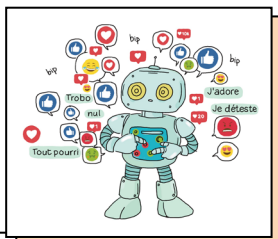
# TECHNIQUES, TACTIQUES ET PROCÉDURES

Les acteurs de la menace ont recours à différentes techniques, tactiques et procédures (TTP) qui sont aujourd’hui bien documentées par VIGINUM et décrites dans ses rapports publics.

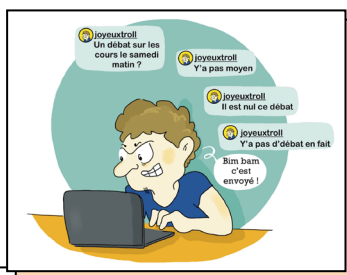
En voici quelques-unes :

**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.

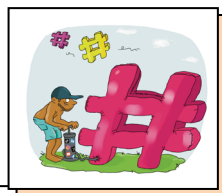
Citons par exemple :



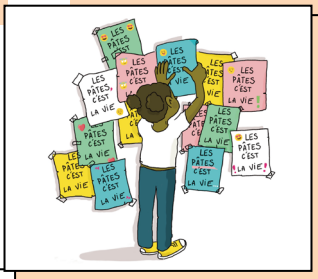
**Les bots** : technique consistant en l’utilisation d’avatars sur les réseaux sociaux, dont la création ou les actions ont été automatisées par un programme informatique pour simuler le comportement d’un être humain. Un bot peut être capable de faire des publications, de laisser des commentaires, de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



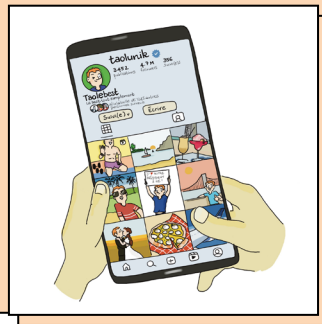
**Les trolls** : comptes ou groupes de comptes derrière lesquels se cachent des personnes réelles qui, par jeu, moquerie, activisme politique ou encore par stratégie, insultent, offensent ou provoquent la polémique sur un sujet afin de déstabiliser le débat public numérique. Contrairement aux bots, les trolls ne sont pas des comptes automatisés.



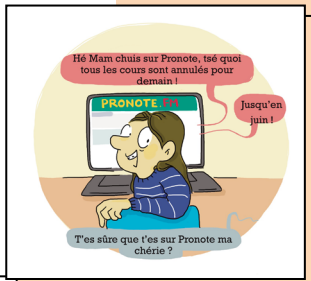
**Astrourfing** : technique consistant à augmenter artificiellement la visibilité d’un sujet par l’action coordonnée d’un groupe restreint de comptes qui vont produire un volume important de publications. Cette technique sert à faire croire qu’un sujet est un phénomène de masse. L’astrourfing a, par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



**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 de légères modifications (émoticônes, ponctuation, etc.) dans le but d'amplifier la visibilité d'un message sans être censuré par les plateformes. Cette technique a été utilisée par le *Baku Initiative Group* dans le cadre de ses opérations informationnelles.



**Spammouflage** : technique caractéristique des acteurs pro-chinois consistant en la diffusion de messages de nature politique dissimulés au milieu de sujets plus anodins (musique, cuisine, sport, *lifestyle*).



**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 attentifs. Le mode opératoire informationnel *RRN* a souvent recours à cette technique.



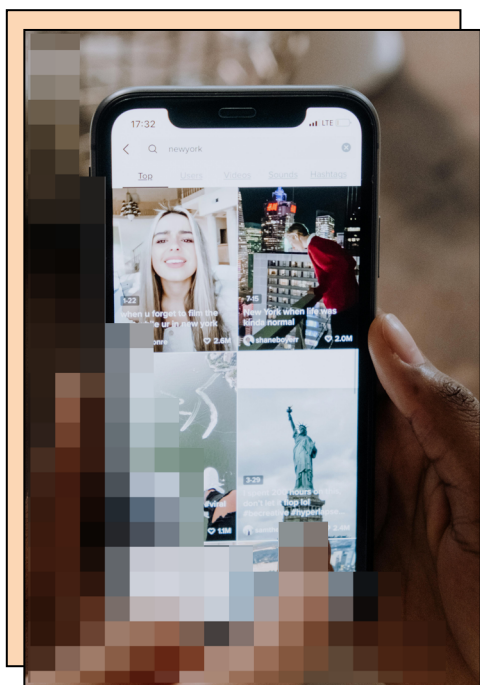
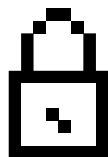
**IA générative** : technique consistant à utiliser des modèles d'intelligence artificielle (IA) générative, capable de créer des contenus (texte, image, vidéo, musique) à partir d'un *prompt* donné à la machine, afin de produire des contenus originaux imitant des réalisations humaines. On pense par exemple à des vidéos de type *deepfake* (« hypertrucage » en français) comme celles créées par le mode opératoire informationnel *Storm-1516*.



**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.

# CONSEILS DE SENSIBILISATION

Face aux manipulations de l'information en ligne, nous sommes tous des cibles potentielles ! Alors, comment s'en protéger ?



## ADOPTONS UNE POSTURE CRITIQUE

Prenons du recul sur l'information consultée, méfions-nous des titres trop accrocheurs ou faisant appel aux émotions et croisons nos sources.

## VÉRIFIONS LE CONTENU DE LA SOURCE

Vérifions l'exactitude des faits et des chiffres énoncés, regardons la date et le contexte de publication de l'article.



## VÉRIFIONS LES IMAGES

Faisons une recherche inversée d'images et de vidéos (*reverse image*) pour déceler si le contenu a déjà été utilisé dans un contexte différent.

## ANALYSONS L'AUTHENTICITÉ DE LA SOURCE

Portons un œil attentif à des éléments du compte qui pourraient témoigner de leur caractère inauthentique : 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), une photo de profil qui semble générée par IA, etc. Ces différents éléments sont caractéristiques de l'action coordonnée de comptes inauthentiques.

## RÉFLÉCHISSONS AVANT DE REPARTAGER

Contribuons à lutter contre la manipulation d'une information en évitant de repartager des contenus douteux.

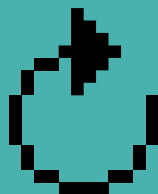
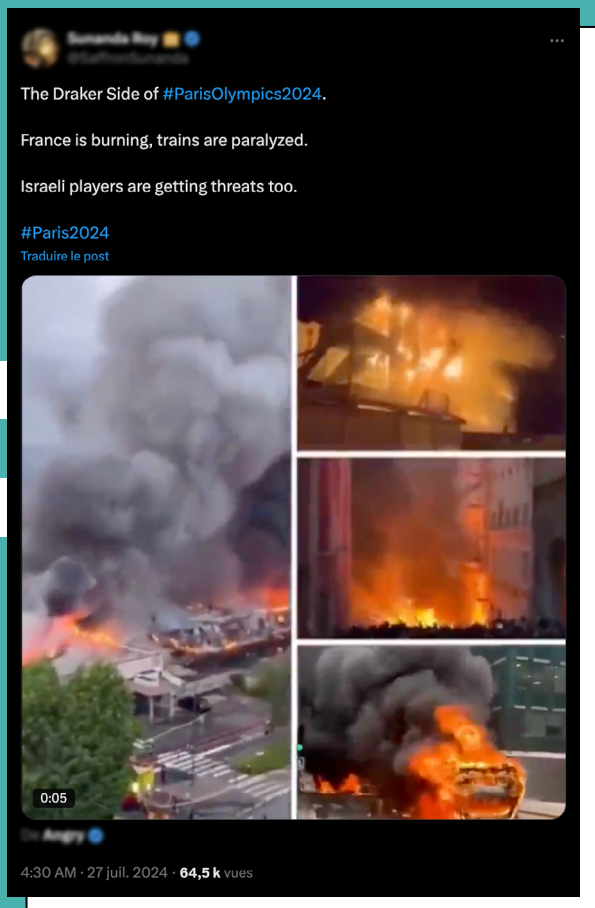
## SIGNALONS DES CONTENUS ILLICITES

Agißons lorsque nous sommes exposés à des contenus illicites en les signalant soit directement aux plateformes concernées, soit auprès de [Pharos](#), le portail officiel de signalement des contenus illicites sur internet.

# TESTER LE « REVERSE IMAGE »

MISSION

Observons ce post trouvé sur la plateforme X.



La légende indique :

« Le côté plus sombre des #JeuxOlympiquesdeParis2024. La France brûle, les trains sont paralysés. Les athlètes israéliens reçoivent aussi des menaces. #Paris2024 »

## QUESTION 01

**Que voit-on sur les photos?**

## QUESTION 02

**Quels sentiments ce post provoque-t-il ?**

Selon la publication, des bâtiments en France seraient en train de brûler pendant les jeux Olympiques et Paralympiques de Paris 2024. L'objectif est de décrédibiliser la France et sa capacité à accueillir les jeux, de décourager les touristes à se rendre en France.

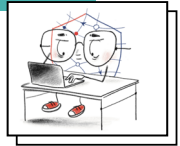
Pourtant, en réalisant un *reverse image*, on comprend que ces images n'ont rien à voir avec les jeux de Paris... Mais sont celles d'un incendie criminel en Seine-et-Marne qui a eu lieu en 2023, suite à des émeutes urbaines! On n'est donc ni dans le thème présenté ni dans la bonne année.

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

Ouvrir l'image dans un nouvel onglet  
Enregistrer l'image sous...  
Copier l'image  
Copier l'adresse de l'image  
Rechercher avec Google Lens

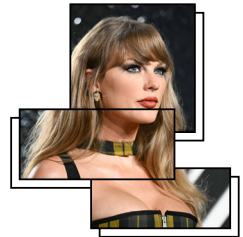
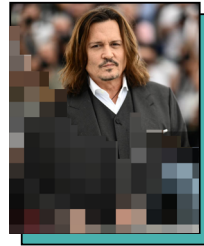
# TESTER SES CONNAISSANCES ENTRE ADULTES ET JEUNES

Êtes-vous prêts à tester votre capacité à identifier les techniques employées pour manipuler des informations? Cet exercice vous invite à partager un moment d'apprentissage conjoint entre adultes et jeunes dans une mission ludique et instructive.



Ensemble, écoutez une série de **8 podcasts mettant en scène Clara et Raphaël**, une sœur et un frère qui expliquent de manière accessible les différentes techniques utilisées par les acteurs malveillants.

À la suite de chaque épisode, trois questions vous seront proposées pour approfondir la compréhension du contenu et en discuter ensemble.



## ÉPISODE 01

### Johnny Depp et l'astroturfing

1. Quel est le sujet des extraits vidéos visionnés par Raphaël?
2. De quelle manière la rumeur a-t-elle été amplifiée sur internet et quel est son but?
3. Comment s'appelle la technique utilisée et en quoi consiste-t-elle?

## ÉPISODE 02

### Les Swifties et l'IA générative

1. Dans quelle démarche s'inscrit cette nouvelle campagne de manipulation de l'information?
2. Quelle est la technique utilisée et comment la détecter?
3. Qu'est-ce qu'un *deepfake* et quel est son objectif?

### ÉPISE 03

## Clara et les typosquatteurs

1. Pourquoi Clara est-elle de très bonne humeur et quel est le cadeau que lui ont fait ses amies ?
2. En quoi consiste la technique et dans quelle mesure est-elle utilisée pour diffuser une fausse information ?
3. Quels sont les bons réflexes à avoir ?

### ÉPISE 04

## Clara et la diffusion sporadique\* de messages politiques

1. Sur quel réseau social se déroule l'action discutée dans cet épisode ?
2. En quoi consiste cette technique ?
3. Quel acteur malveillant utilise fréquemment cette technique ?

### ÉPISE 05

## Raphaël et les influenceurs roumains

1. Dans quel contexte s'inscrit cette nouvelle manœuvre informationnelle et quel acteur est impliqué ?
2. Que permet le recrutement d'influenceurs et quel a été le résultat de cette manœuvre informationnelle ?
3. Dans quel contexte cette technique a-t-elle été utilisée en France ?

### ÉPISE 06

## Blake Lively et les bots

1. Quel est le sujet de l'enquête de Raphaël ?
2. Qu'est-ce qu'un bot ?
3. Quelle est la technique qui implique l'utilisation de bots et comment la détecter ?

### ÉPISE 07

## Dans ton algorithme

1. Quel est le but des algorithmes des réseaux sociaux ?
2. En quoi les algorithmes peuvent-ils être instrumentalisés à des fins politiques ?
3. Quel est l'impact de la suspension de la modération sur les réseaux sociaux, c'est-à-dire le contrôle et le tri des contenus sur les réseaux sociaux pour éviter les messages dangereux, insultants ou faux ?

### ÉPISE 08

## Arrête de troller !

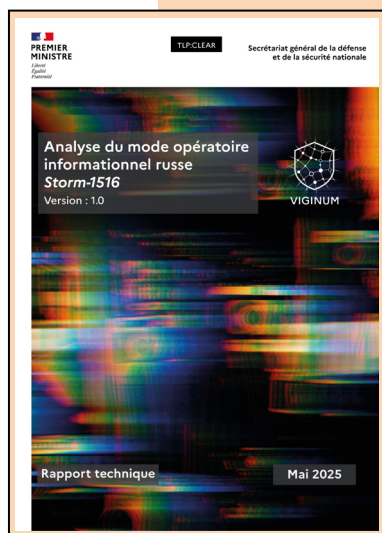
1. Qu'est-ce qu'un troll ?
2. Quelle est la différence entre des bots et des trolls ?
3. Comment les trolls sont-ils utilisés dans un but politique ?

\* Une diffusion sporadique désigne une situation où quelque chose (comme une information, une maladie ou un message) se propage ou apparaît seulement de temps en temps, de manière irrégulière. Cela ne suit pas un rythme régulier et peut arriver n'importe quand.

## RAPPORTS

# À LA DÉCOUVERTE DU RAPPORT « STORM-1516 »

Après plusieurs mois d'enquête, VIGINUM a publié en mai 2025 **un rapport** portant 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.



## QUELS SONT LES OBJECTIFS DE STORM-1516?

- **Cibler 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.
- **Cibler les intérêts occidentaux** : *Storm-1516* cherche aussi à décrédibiliser des dirigeants ou des proches de personnalités politiques européennes ou américaines.
- **Cibler 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.

## QUELLES SONT LES TECHNIQUES EMPLOYÉES ?

*Storm-1516* utilise une grande variété de procédés pour produire des contenus et diffuser des informations manipulées vers le plus grand nombre :

- **des montages photos et vidéos** : ceux-ci visent à contrefaire des logos de médias, des affiches de films, des registres publics, des documents gouvernementaux, des factures, des articles de presse ou encore des captures d'écran de réseaux sociaux, et ce, afin de crédibiliser les narratifs trompeurs/erronés qui sont diffusés ;
- **des vidéos impliquant des acteurs amateurs** : de vraies personnes sont recrutées pour enregistrer des voix *off*, jouer un rôle de lanceur d'alerte ou intervenir dans une mise en scène ;
- **des vidéos et audios probablement générés par IA** : l'IA permet de mettre en scène des individus à visage découvert en modifiant leur visage, et non plus des acteurs apparaissant face cachée, mais aussi d'usurper l'identité de personnalités publiques et d'internautes.



## STORM-1516 A-T-IL UN IMPACT SUR LE DÉBAT PUBLIC ?

Si l'impact réel sur le débat public numérique est difficile à estimer, une grande partie des contenus diffusés ont 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.

# MISSION

Les informations manipulées ci-dessous ont été diffusées en ligne par le MOI Storm-1516.

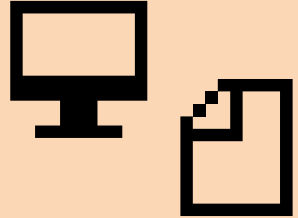
Sauriez-vous associer le procédé utilisé à l'image correspondante ?

Les techniques employées :

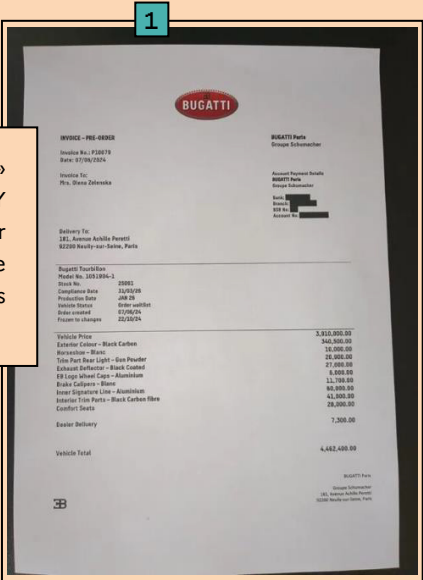
Vidéo générée par IA/deepfake **A**

Photomontage **B**

Recrutement d'un acteur amateur pour tourner dans un faux reportage **C**



La photo d'une facture « prouverait » que la femme de Volodymyr ZELENSKY a profité d'une visite en France pour acheter une voiture de la marque Bugatti, d'un montant de 4,5 millions d'euros.

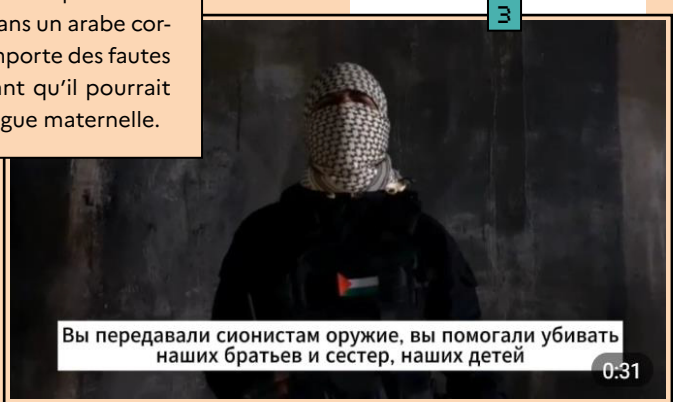


Réponses : A-2/B-1/C-3



Dans un témoignage vidéo, un individu accuse le colistier de Kamala HARRIS, Timothy WALTZ, d'avoir agressé sexuellement un de ses anciens élèves en 1997. Les traits de l'individu semblent avoir été « usurpés » pour recréer son visage, potentiellement à partir de photos issues de ses réseaux sociaux.

Quelques jours avant la cérémonie d'ouverture des jeux Olympiques de Paris 2024, une vidéo publiée sur X, Facebook et Telegram met en scène un prétendu membre du Hamas menaçant la France et dénonçant la participation d'athlètes israéliens à la compétition. Si l'individu s'exprime dans un arabe correct, son discours comporte des fautes d'intonation, suggérant qu'il pourrait ne pas s'agir de sa langue maternelle.



## RAPPORTS

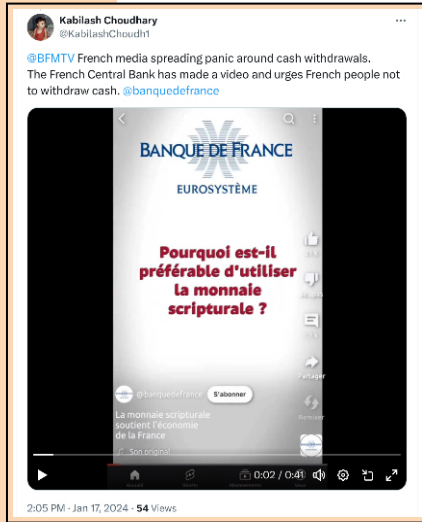
# À LA DÉCOUVERTE DU RAPPORT « MATRIOCHKA »

En juin 2024, VIGINUM a publié **un rapport** sur **la campagne Matriochka** dont les actions se poursuivent encore après la publication.



## MATIOCHKA, QU'EST-CE QUE C'EST ?

*Matriochka* est un mode opératoire informationnel russe, susceptible d'affecter le débat public francophone. Documenté par VIGINUM depuis la fin de l'année 2023, ce MOI s'appuie sur la publication de faux contenus, tels que des reportages, des mèmes ou des graffitis dans le champ physique, et qui font ensuite l'objet d'une diffusion coordonnée, notamment dans l'espace « Réponse » de publications sur les comptes X (ex-Twitter) de médias, de *fact-checkers* ou de personnalités. Les acteurs malveillants derrière cette campagne les interpellent ainsi directement pour leur demander d'enquêter sur de faux contenus. L'objectif de cette campagne est de décrédibiliser les entités interpellées tout en promouvant des contenus favorables aux intérêts russes, mais aussi de placer le sujet de la désinformation russe au cœur de l'agenda médiatique.



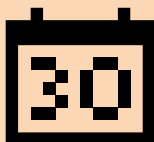
**Fact-checker** : un *fact-checker* ou un vérificateur de faits est une personne chargée de vérifier l'exactitude des informations énoncées grâce à différentes techniques.

## QUELLES SONT LES TECHNIQUES UTILISÉES ?

Les opérateurs de *Matriochka* ont utilisé différentes techniques. L'une d'entre elles consistait à diffuser des informations manipulées (faux graffitis, vidéos, captures d'écran, documents officiels) en usurpant l'identité et la charte graphique de médias, d'organisations gouvernementales ou d'ONG. Par ailleurs, les opérateurs ont aussi utilisé la technique du *copy pasta*, qui consiste à copier-coller des messages trompeurs pour amplifier leur visibilité sur les réseaux sociaux. Les messages diffusés ont prioritairement visé l'Ukraine et son gouvernement pour les décrédibiliser et affaiblir le soutien occidental.

## ET LA FRANCE DANS TOUT ÇA ?

Si de nombreux pays ont été ciblés par *Matriochka*, la France constitue une cible privilégiée, en raison de son engagement en faveur de l'Ukraine. Des médias français, à l'instar de BFM TV, du *Monde* ou encore du *Parisien*, ont vu leur identité usurpée. En outre, de nombreux graffitis ont été présentés comme étant situés en région parisienne. L'idée est de créer une défiance envers les institutions françaises, mais aussi de décrédibiliser l'organisation des jeux Olympiques et Paralympiques 2024. Depuis la publication de son rapport technique, VIGINUM a vu son identité usurpée par *Matriochka* à plusieurs reprises.

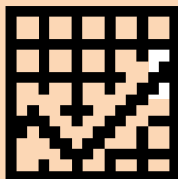


## MISSION

À partir du visionnage de **ce reportage** réalisé par la cellule de *fact-checking* Les Vérificateurs de TF1, pourriez-vous expliquer dans quelle mesure *Matriochka* vise à jeter le discrédit sur le travail des cellules de *fact-checking* et le but recherché par ses opérateurs ?

Et vous, êtes-vous familier avec les cellules de *fact-checking* ?

Consultez-vous les services proposés par vos médias du quotidien ?





## RAPPORTS

# À LA DÉCOUVERTE DU RAPPORT SUR LES ÉLECTIONS EN ROUMANIE

En février 2025, VIGINUM a publié **un rapport** pour tirer des enseignements des élections présidentielles roumaines de 2024. Celui-ci revient sur les manipulations de l'information ayant ciblé cette élection, dont les résultats du premier tour ont été annulés par la Cour constitutionnelle roumaine. VIGINUM en profite pour sensibiliser les internautes sur deux techniques de manipulation de l'information observées à cette occasion : la manipulation des algorithmes de recommandation des réseaux sociaux, notamment *TikTok*, et l'instrumentalisation d'influenceurs.



### LA MANIPULATION DE L'ALGORITHME DE TIKTOK

Il est aujourd'hui relativement facile d'imposer aux utilisateurs la visibilité d'un sujet sur un réseau social tel que *TikTok*. Comme observé lors des élections roumaines, plusieurs milliers de comptes peuvent être coordonnés pour publier massivement des vidéos et des commentaires comportant certains *hashtags* et mots-clés liés à un candidat. Ce procédé, appelé *astroturfing*, contribue à manipuler l'algorithme de recommandation, en générant artificiellement une tendance émergente autour d'un sujet (en l'occurrence ici, un candidat et son programme).



## L'INSTRUMENTALISATION D'INFLUENCEURS

Dans le contexte de l'élection roumaine, plus d'une centaine d'influenceurs *TikTok*, sans affinité particulière avec la politique, ont été instrumentalisés pour donner de la visibilité à un candidat. Contactés *via* des plateformes de marketing d'influence permettant de mettre facilement en relation des annonceurs avec des nano- et micro-influenceurs, ils ont accepté l'offre qui leur était faite sans toutefois connaître l'identité des entreprises qui les contactaient, ni le commanditaire ou l'objectif réel de la campagne. La mécanique a consisté à leur faire publier des messages d'apparence anodine, relatifs à l'élection présidentielle, avant de créer artificiellement, *via* les commentaires sous leurs vidéos, un engagement coordonné visant à promouvoir le candidat et son programme.

## QUELLES LEÇONS POUR LA FRANCE ?

Bien que l'audience et les usages de *TikTok* diffèrent entre la Roumanie et la France, le public français est présent et actif sur cette plateforme. Des acteurs étrangers malveillants pourraient donc être tentés de choisir *TikTok* pour mettre en œuvre le même schéma opérationnel qu'en Roumanie, que ce soit pour déstabiliser un rendez-vous électoral ou pour faire émerger des thématiques spécifiques dans le débat public.

## MISSION

Pour chaque phrase, retrouvez le mot manquant :

Mots manquants :  ,  ,  ,  ,  .

Le rapport évoque une campagne d'  , visant à faire croire à un soutien populaire spontané alors qu'il est artificiel.

Des vidéos ont été massivement commentées pour manipuler l'  de *TikTok*.

Des  ont été recrutés à leur insu pour relayer des contenus influents.

Des réseaux de comptes coordonnés ont été activés *via* des applications comme  pour diffuser des instructions et des contenus.

Pour renforcer l'impact des vidéos, certains influenceurs ont utilisé des  populaires comme *#Prezidentiale2024* ou *#unliderpotrivitpentrumine*.

Réponses : *astroturfing* / *algorithme* / *hashtags* / *influenceurs* / *Telegram*

# NOS CONTENUS DE SENSIBILISATION

## LA FICHE PÉDAGOGIQUE EDUC'ARTE

### Comprendre et déjouer les mécanismes de manipulation de l'information avec VIGINUM et Educ'ARTE

VIGINUM a collaboré avec la plateforme Educ'Arte afin de produire une fiche pédagogique sur les manipulations de l'information. Celle-ci est composée d'éléments de contexte, d'une sélection de vidéos et d'exemples d'activités à réaliser en classe, ainsi que de « fiches métiers ». Cette fiche s'adresse principalement aux enseignants du secondaire (collège et lycée) afin de les encourager à se saisir des enjeux de la manipulation de l'information et à sensibiliser leurs élèves.



THE  
OSINT  
PROJECT

### Comprendre et déjouer les mécanismes de manipulation de l'information avec VIGINUM



DISCIPLINES : EMC, EMI, EMC-Anglais  
NIVEAUX : Collège (Lycée Al, Seconde, Première, Terminale)

Thème avec les programmes scolaires :

- Responsabilités, libertés et droits fondamentaux - Libertés d'expression et de la presse, notamment en ligne.
- Éducation à la détection : online public, souveraineté numérique, sécurité nationale, cybercriminalité.
- Faire la guerre, faire la paix - Formes de conflits et modes de résolution, la notion de guerre hybride.
- L'enjeu de la connaissance : la cybersécurité, la cybersociété.
- Certification PIX et CRCN.

Objectifs / compétences :

- **Prévenir** les risques numériques.
- **Analyser** l'information : adopter une démarche réflexive.
- Faire preuve de discernement et exercer son esprit critique.
- **Se documenter**.
- **Travailler** de manière autonome et / ou en groupe.
- **Déterminer** à l'oral ou à l'écrit.
- **Développer** un sentiment d'appartenance à une communauté.
- **Résister** à ses autres et soi-même.
- **Résoudre** des conflits et / ou prendre des décisions.

Mots clés :

- liberté d'expression, droits fondamentaux, défense (l'ortique), guerre informationnelle, guerre hybride, sécurité, cybersociété, désinformation, manipulation, mensonge, deepfake, souveraineté nationale, diplomatie, ingénierie, géopolitique, réseaux sociaux, communication, bases nouvelles (base news info), effets des médias, question d'actualité, citoyen transparent.

#### PRÉSENTATION DE VIGINUM

VIGINUM est le service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères (INIE) au sein des services du Premier ministre. Créé en 2021, il répond à son rôle majeur : protéger la sécurité publique, l'information contre les campagnes numériques de manipulation de l'information impliquant des acteurs étrangers, qui sont de nature à nuire à la France et à ses intérêts.

**Service d'investigation en ligne** VIGINUM a comme mission principale de détecter et de caractériser les opérations d'ingérence numériques étrangères, à la recherche de **signes certains** :

- une volonté de porter atteinte aux intérêts fondamentaux de la Nation ;
- un contenu intentionnellement faux et trompeur ;
- une affiliation artificielle ou automatisée, massive et déstabilisante ;
- l'implication, directe ou indirecte, d'un acteur étranger (individu, organisation ou non-déclaré).

Pour ce faire, VIGINUM travaille exclusivement à partir de **contenus publiquement accessibles sur les plateformes en ligne, sites web et médias web** afin de limiter ses interventions, respectant aux quatre critères mentionnés précédemment. Les équipes ont recours aux **techniques OSINT** (Open source intelligence) pour mener leurs investigations.

Au titre de ses attributions, VIGINUM est également investi d'une **mission particulière en matière de sécurité** afin d'assurer la protection de ces données recueillies dans le champ informationnel. Durant cette période, VIGINUM rend compte aux autorités garanties du bon fonctionnement des élections de toute information liée à l'accomplissement de leurs missions. Outre la sécurisation des sources électroniques, le service est également mobilisé pour protéger le **débat public numérique** ainsi que garantir le traitement de la sécurité informationnelle susceptible d'être instrumentalisée par des **acteurs étrangers malveillants**.

Plus d'informations sur le **OSINT** en cliquant sur :



Ministère de l'Intérieur  
Ministère national de la Sécurité intérieure

## LES 3 CHALLENGES OSINT SUR LA PLATEFORME TOP

En partenariat avec le Campus Cyber, VIGINUM s'est associé à la plateforme *The Osint Project (TOP)* pour créer **trois nouveaux challenges OSINT sur les manipulations de l'information et les ingérences numériques étrangères**. S'inspirant de cas concrets observés en investigation, les challenges permettent de découvrir les principales techniques d'OSINT par des moyens ludiques et pédagogiques. Différents niveaux de difficulté sont proposés afin de s'adresser au plus grand nombre. À destination des 12-18 ans, la plateforme est accessible à tous sur inscription.

## Pour découvrir l'ensemble des rapports de VIGINUM



### LE PODCAST « LE DÉBRIEF DE CLARA ET RAPHAËL »

#### Le débrief de Clara et Raphaël : Comment débusquer les manipulations de l'information – DE FACTO – Des clés pour mieux s'informer

VIGINUM et le centre pour l'éducation aux médias et à l'information (CLEMI), service du réseau Canopé, se sont associés pour créer le *podcast* fictionné « Le débrief de Clara et Raphaël ». Il se compose de 8 épisodes, chacun présentant une technique utilisée par les acteurs malveillants, dans le cadre de manœuvres de manipulation de l'information. À destination des enseignants et des jeunes publics, ce *podcast* est accompagné d'une mallette de ressources pédagogiques réunissant des fiches pédagogiques produites par le CLEMI. L'initiative s'inscrit dans le cadre du projet européen DE FACTO, mis en ligne à l'occasion de la semaine de la presse et des médias 2025 organisée par le CLEMI. Cette série de *podcasts* est disponible sur toutes les plateformes d'écoute.



### LE MODULE DE FORMATION « DÉSINFORMATION ET INGÉRENCES NUMÉRIQUES ÉTRANGÈRES »

VIGINUM et le CLEMI lancent un parcours de formation inédit à destination des enseignants du second degré, **disponible dès à présent sur la plateforme Magistère**. Cette ressource innovante vise à renforcer les compétences des enseignants face aux manipulations de l'information et à leur fournir des outils concrets pour préparer les élèves à y faire face avec discernement et esprit critique.

# CORRECTION DES JEUX

## MISSION

### TESTER SES CONNAISSANCES ENTRE ADULTES ET JEUNES

#### ÉPISODE 1 : JOHNNY DEPP ET L'ASTROTURFING

1. Les extraits vidéos portent sur la campagne de manipulation de l'information orchestrée autour du célèbre procès opposant Amber Heard et Johnny Depp, deux acteurs américains.
2. Des acteurs malveillants ont diffusé ces fausses informations à leurs communautés, qui se sont empressées de les repartager sur les réseaux sociaux et notamment sur X (ex-Twitter). Le but de cette manœuvre est d'affaiblir le soutien à Amber Heard et de décrédibiliser sa défense lors du procès.
3. *Astroturfing* : cf. pages Techniques, tactiques et procédures.

#### ÉPISODE 2 : LES SWIFTIES ET L'IA GÉNÉRATIVE

1. L'objectif visé par les acteurs malveillants est de faire croire que les fans de Taylor Swift sont des partisans de Donald Trump.
2. IA générative : cf. pages Techniques, tactiques et procédures.
3. Un *deepfake* est une image, une vidéo ou un enregistrement sonore créé avec un ordinateur, qui imite très bien le visage ou la voix de quelqu'un. Grâce à cette technologie, on peut faire croire qu'une personne a dit ou fait quelque chose, alors que ce n'est pas vrai.

#### ÉPISODE 3 : CLARA ET LES TYPOSQUATTEURS

1. Clara est de très bonne humeur, car ses amies lui ont fabriqué une fausse Une du journal sportif *L'Équipe* sur laquelle elle est sacrée Ballon d'or.
2. *Typosquatting* : cf. pages Techniques, tactiques et procédures.
3. Pour éviter d'être victime d'une manœuvre de *typosquatting*, il est essentiel de toujours vérifier l'adresse du site et si l'information a été reprise ailleurs par d'autres médias.

#### ÉPISODE 4 : CLARA ET LA DIFFUSION SPORADIQUE DE MESSAGES POLITIQUES

N.B. : Une diffusion sporadique désigne une situation où quelque chose (comme une information, une maladie ou un message) se propage ou apparaît seulement de temps en temps, de manière irrégulière. Cela ne suit pas un rythme régulier et peut arriver un peu n'importe quand.

1. L'action se déroule sur le réseau social *Instagram*.
2. *Copy pasta* : cf. pages Techniques, tactiques et procédures.
3. La Chine.

## ÉPISEDE 5 : RAPHAËL ET LES INFLUENCEURS ROUMAINS

1. Cette nouvelle manœuvre informationnelle est survenue lors des élections présidentielles roumaines fin 2024. Elle implique un candidat à l'élection présidentielle ayant fait campagne exclusivement sur le réseau social *TikTok*.
2. Les acteurs malveillants ont manipulé l'algorithme de *TikTok* avec de multiples faux comptes, tout en recrutant des influenceurs roumains pour faire passer des messages politiques en faveur du candidat d'extrême droite Calin Gorgescu.
3. Le recrutement d'influenceurs permet d'utiliser des comptes disposant d'une forte audience pour amplifier la diffusion d'un contenu et bénéficier d'une audience plus large. Par ailleurs, les influenceurs prêtent leur légitimité et leur crédibilité aux émetteurs des messages. Le résultat a été l'annulation du premier tour des élections présidentielles roumaines.

## ÉPISEDE 6 : BLAKE LIVELY ET LES BOTS

1. Raphaël explique à sa sœur qu'il s'est passionné pour une affaire impliquant l'actrice américaine Blake Lively sur le tournage d'un film intitulé *Jamais Plus*. Cette dernière a été victime d'une attaque réputationnelle orchestrée par le réalisateur du film, à la suite d'un différend sur des accusations de propos sexistes.
2. *Bots* : cf. pages Techniques, tactiques et procédures.
3. *Copy pasta* : cf. pages Techniques, tactiques et procédures.

## ÉPISEDE 7 : DANS TON ALGORITHME

1. Le but des algorithmes des réseaux sociaux est de nous montrer des contenus (vidéos, photos, messages) que l'on aime ou que l'on trouve intéressants afin de passer beaucoup de temps sur l'application.
2. Les algorithmes sont conçus pour favoriser de l'engagement et montrent par conséquent les contenus les plus extrémistes, car ils génèrent des commentaires, des *likes* et des partages.
3. La suspension de la modération signifie que les contenus diffusant de la désinformation, des messages haineux ou extrémistes sont susceptibles de circuler librement sur les réseaux sociaux.

## ÉPISEDE 8 : ARRÊTE DE TROLLER !

1. *Trolls* : cf. pages Techniques, tactiques et procédures.
2. Les *bots* sont automatisés, ce qui n'est pas le cas des *trolls*.
3. Les *trolls* permettent de diffuser des messages pro-gouvernementaux et décrédibiliser les adversaires politiques.



VIGINUM

Secrétariat général de la défense  
et de la sécurité nationale

**Conception**

VIGINUM

La Netscouade

**Impression**

Imprimerie Baudelaire

Février 2026

VIGINUM\_Academie\_LMI@sgdsn.gouv.fr

**Crédits iconographiques**

AFP, Pexels, Freepik, Véropée