



# Présentation du service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères (VIGINUM) - Grand entretien

Publié le 14 octobre 2024

Dans un environnement numérique en constante évolution, Viginum a pour vocation de protéger l'intégrité de l'information et prévenir les manipulations en ligne. Dans cet échange, le service nous explique ses missions, les défis auxquels il est confronté et les stratégies adoptées pour assurer la fiabilité des informations diffusées sur Internet.

*Entretien réalisé en mai 2024.*



## Quelle est la genèse de VIGINUM ?

Pour le public français, la menace des ingérences numériques étrangères s'était faite lors de l'affaire des "Macron Leaks" en 2017, épisode au cours duquel l'élection présidentielle française avait fait l'objet d'une manœuvre hostile mêlant à la fois cyberattaque et manipulation de l'information. Malheureusement, à l'automne 2020, la menace

## **Présentation du service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères (VIGINUM) -**

### **Grand entretien - IH2EF - Page 2**

informationnelle s'est durcie, répandue et intensifiée. À la suite de l'assassinat de Samuel Paty, la France a été la cible d'une vaste et violente campagne de dénigrement sur les réseaux sociaux.

Ainsi, au mois de novembre 2020, les autorités françaises ont décidé de confier au Secrétariat général de la défense et de la sécurité nationale (SGDSN) le pilotage d'un groupe de travail, la taskforce "Honfleur", chargé de mieux comprendre les phénomènes de propagation des contenus anti-français sur les plateformes numériques et de proposer le cas échéant une réponse adaptée. À l'issue de ses analyses, la taskforce "Honfleur" a conclu qu'une part importante des expressions hostiles à la France et à son modèle démocratique était bien le résultat d'activités inauthentiques produit par un nombre restreint de comptes, probablement inspirés voire orchestrés par des acteurs étrangers. Face à ce constat, une mission de préfiguration, succédant à la taskforce "Honfleur", a alors été mise en place au début de l'année 2021.

À la suite de travaux préparatoires impliquant de nombreuses consultations, le décret n° 2021-922 du 13 juillet 2021 a modifié les dispositions du Code de la défense en dotant le SGDSN de nouvelles attributions en matière de lutte contre les ingérences numériques étrangères. Pour l'assister dans l'exercice de ces nouvelles missions, ce décret a créé un service à compétence nationale chargé de la vigilance et de la protection contre les ingérences numériques étrangères (VIGINUM). Ce nouveau service, placé auprès du SGDSN, est chargé de détecter et caractériser les opérations d'ingérences numériques étrangères aux fins de manipulation de l'information sur les plateformes en ligne.



### **Qu'est-ce qu'une ingérence numérique étrangère selon la définition opérationnelle de VIGINUM ?**

Au sens du [décret n° 2021-922 du 13 juillet 2021](#) portant création du service VIGINUM, une ingérence numérique étrangère est une opération ou une campagne malveillante, se tenant sur les plateformes en ligne et constituée par quatre critères :

- une volonté de porter atteinte aux intérêts fondamentaux de la Nation ;
- un contenu manifestement inexact ou trompeur ;
- une diffusion artificielle ou automatisée, massive et délibérée ;
- l'implication, directe ou indirecte d'un acteur étranger (étatique, paraétatique ou non-étatique).



### **Pouvez-vous décrire les missions de VIGINUM pour protéger le débat public ?**

En tant qu'administration en charge d'une mission défensive, la détection et la caractérisation des ingérences numériques étrangères, VIGINUM fait figure d'exception.

## **Présentation du service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères (VIGINUM) -**

### **Grand entretien - IH2EF - Page 3**

Service d'investigation en ligne, VIGINUM s'attache avant tout à analyser les comportements, modes opératoires et infrastructures utilisés par les acteurs étrangers malveillants pour diffuser des contenus attentatoires aux intérêts fondamentaux de la Nation.

Pour ce faire, le service travaille exclusivement à partir de contenus publiquement accessibles sur les plateformes en ligne, sites web et médias web afin de mettre en évidence les phénomènes répondant aux quatre critères mentionnés précédemment.

Au titre de ses attributions, il est également investi d'une mission particulière en période électorale afin d'assurer la protection de ces grands rendez-vous. Durant cette période, il rend compte aux autorités garantes du bon déroulement des élections de toute information utile à l'accomplissement de leurs missions.

Outre la sécurisation des scrutins électoraux, le service est également mobilisé pour protéger le débat public numérique en réaction à de grands événements de l'actualité internationale susceptibles d'être instrumentalisés par des acteurs étrangers malveillants.



### **Pouvez-vous décrire la combinaison particulière d'expertises de l'équipe de VIGINUM afin de lutter contre les ingérences numériques ?**

Le service est aujourd'hui composé d'une cinquantaine d'agents. Il s'appuie sur une équipe pluridisciplinaire composée de spécialistes en investigation et analyse numériques (Open Source INTelligence, information en sources ouvertes - OSINT ), d'experts en marketing digital et de spécialistes en sciences politique et géopolitique.

Le service possède également un Datalab composé de data scientists et de data ingénieurs spécialisés dans l'analyse et le traitement de données. Il travaille main dans la main avec les analystes afin de les appuyer techniquement à déterminer le caractère d'ingérence numérique étrangère (INE) d'une campagne à partir des jeux de données. Il maintient également une activité recherche et développement (R&D) afin de maintenir le service à l'état de l'art tout en ouvrant ce dernier vers le monde académique via la rédaction d'articles scientifiques de haut niveau et la participation à des conférences.



### **Comment VIGINUM garantit-elle son fonctionnement avec expertise, objectivité et coopération et pourquoi ces valeurs sont-elles centrales à sa mission ?**

Par nature sensible, l'activité opérationnelle de VIGINUM doit être strictement encadrée. Aussi, le service est accompagné par un comité éthique et scientifique placé auprès du SGDSN pour suivre son activité opérationnelle. Il est présidé par un représentant du Conseil d'État et rassemble des personnalités qualifiées dans les domaines de la diplomatie, de l'application de la loi, de la science et des médias. Ce comité est rendu destinataire de toute

## **Présentation du service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères (VIGINUM) -**

### **Grand entretien - IH2EF - Page 4**

information relative à la mise en œuvre des missions du service, à qui il peut adresser, en tant que de besoin, des recommandations. Il assure à la fois une fonction de conseil et, pour demain, de liaison avec notamment une communauté scientifique riche de talents, active et experte dans les champs de la lutte contre les manipulations de l'information (LMI).

L'ensemble de ces observations et réflexions font l'objet d'un rapport annuel publié sur le site du SGDSN.



### **Comment VIGINUM navigue-t-elle dans la collecte de données personnelles d'une manière qui respecte les cadres légaux et les droits individuels ? Pourriez-vous détailler (succinctement) les plateformes à partir desquelles VIGINUM est autorisée à collecter des données publiquement accessibles et les critères guidant cette collecte ?**

L'activité opérationnelle de VIGINUM s'inscrit dans un cadre juridique et éthique unique. En effet, la création du service, par le [décret n° 2021-922 du 13 juillet 2021](#), garantit en premier lieu un principe de transparence quant à l'action de l'État pour protéger le débat public contre toute tentative d'interférence par des acteurs étrangers malveillants, notamment lors des rendez-vous démocratiques. Tout citoyen peut le consulter et y trouver des informations utiles sur les missions exercées.

En outre, VIGINUM est autorisé, en vertu du [décret n° 2021-1587 du 7 décembre 2021](#) pris en Conseil d'État après avis de la Commission nationale de l'informatique et des libertés (CNIL), à mettre en œuvre un traitement automatisé de données à caractère personnel dans le but d'identifier les ingérences numériques étrangères. Dans le cadre de ses activités, le service peut donc collecter de manière automatisée certaines catégories de données publiquement accessibles sur les plateformes de plus de 5 millions de visiteurs uniques par mois sur le territoire français. Cela correspond aux plus grandes plateformes connues comme X, Facebook, Instagram, etc.



### **Avez-vous identifié des menaces particulières ou spécifiques visant les intérêts scientifiques, économiques, industrielles, si oui comment VIGINUM y répond ?**

L'exacerbation des tensions internationales favorise une compétition et une mise en concurrence accrues en matière économique. Celles-ci se traduisent dans le champ informationnel par des manœuvres malveillantes, portées par des acteurs étatiques ou non-étatiques, cherchant à porter atteinte aux intérêts économiques incarnés par nos entreprises et à produire des effets dans la vie réelle. Cette menace informationnelle peut se manifester par des actions planifiées ou opportunistes, diffusant de fausses informations ou contribuant à amplifier des critiques et contenus hostiles existants afin de leur conférer davantage de visibilité. Derrière des modes opératoires simples (bots, trolls, usurpation d'identité, raids

## **Présentation du service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères (VIGINUM) -**

### **Grand entretien - IH2EF - Page 5**

numériques), les acteurs étrangers de la menace informationnelle font peser à la fois un risque réputationnel et un risque économique sur nos entreprises.

Concrètement, à la faveur des conflits actuels (Russie-Ukraine et Israël/Hamas), certaines grandes entités économiques ou industrielles françaises ont pu être ciblées par des campagnes de dénigrement et d'appels au boycott sur les réseaux sociaux, plus particulièrement sur X, espace propice aux polémiques sociétales, à la viralisation des contenus et aux mobilisations. Le service observe également l'émergence de nouvelles pratiques sur d'autres plateformes à l'instar de Tik-Tok dans la diffusion de fausses informations liées aux entreprises françaises.

VIGINUM adopte une posture de vigilance pour détecter et documenter la menace informationnelle pesant sur les intérêts économiques, scientifiques et industriels majeurs français. En parallèle de son activité opérationnelle, le service entretient de nombreux contacts avec d'autres ministères ou institutions dont les prérogatives pourraient les conduire à se saisir d'enjeux relatifs à la lutte contre les manipulations de l'information. Tel est le cas du ministère de l'Économie, avec lequel VIGINUM travaille conjointement dans le cadre de la protection des entreprises et des intérêts économiques français face aux tentatives d'ingérences numériques étrangères. Nous nous attachons également à développer des démarches de sensibilisation ainsi que d'accompagnement préventif des entités sensibles.



### **En regardant vers l'avenir, comment VIGINUM envisage de mener des actions de sensibilisation et de formation à la désinformation pour les citoyens en général, pour les enfants et les jeunes gens en particulier ?**

Menace hybride par nature, la manipulation de l'information nécessite une approche globale pour pouvoir y répondre, notamment s'agissant du volet résilience de la société. En la matière, le service investit quatre axes pour améliorer la sensibilisation du grand public.

Depuis le mois de juin 2023, en étroite coopération avec ses partenaires ministériels, le service a directement contribué à révéler publiquement plusieurs campagnes de manipulation de l'information impliquant des acteurs étrangers et susceptibles de porter atteinte aux intérêts fondamentaux de la Nation, dont le réseau "RRN", l'opération dite des "étoiles de David", la campagne de dénigrement des Jeux olympiques (JO) baptisée "Olimpiya", le dispositif "Portal Kombat", le faux site de recrutement pour l'armée de Terre "s'engager-Ukraine". La publication de rapports techniques exposant les modes opératoires utilisés par les acteurs étrangers de la menace informationnelle constitue actuellement une réponse efficace au besoin d'information du public (en France comme à l'international) sur les procédés de manipulation des processus démocratiques. Aussi, le service sera appelé à publier davantage de rapports techniques dans les prochains mois.

## **Présentation du service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères (VIGINUM) -**

### **Grand entretien - IH2EF - Page 6**

Par ailleurs, nous entamons une démarche de rapprochement avec les acteurs de la société civile, notamment le monde académique et scientifique, afin de partager la connaissance sur la menace informationnelle et contribuer au renforcement de l'expertise française. À cet effet, le service a organisé, en juin 2023 son premier colloque académique ouvert au public, aux médias et aux chercheurs. Le succès rencontré pour cette première occurrence a incité le SGDSN (dont relève VIGINUM) à maintenir ce rendez-vous d'ouverture en l'organisant désormais annuellement.

En outre, la présence croissante des ingérences numériques étrangères dans tous les champs du débat public invite à soutenir activement le remarquable travail d'information et de sensibilisation des jeunes publics réalisé par les acteurs des mondes éducatifs, culturels et audiovisuels. En 2024, en étroite liaison avec le ministère de l'Éducation nationale, les médias et la société civile, VIGINUM accompagne d'ores et déjà plusieurs projets éducatifs innovants autour de l'information et de l'éducation aux médias afin de renforcer la vigilance des plus jeunes. À cet effet, il s'agira principalement de produire des contenus et outils à vocation pédagogique en s'appuyant notamment sur des cas d'usage concrets. Enfin, afin de cibler les décideurs, le service a également entamé une démarche de sensibilisation au profit des cadres dirigeants de l'État et du monde de l'entreprise, notamment au travers des cycles de séminaire de l'Institut des hautes études de défense nationale (IHEDN), de l'Institut des hautes études du ministère de l'Intérieur (IHEMI), des écoles et universités et auprès du Mouvement des Entreprises de France (MEDEF).



## **Quels conseils et bonnes pratiques pourraient être mis en place afin de prévenir et lutter contre les campagnes de manipulation de l'information ?**

La conjoncture invite à parfaire le travail d'information et de sensibilisation auprès des utilisateurs d'internet afin d'élever leur niveau de vigilance et de préparation aux défis posés par la menace informationnelle et aux moyens de s'en prémunir.

Quelques recommandations :

- sensibiliser vos collaborateurs sur la réalité de la menace informationnelle et ses différentes manifestations sur les réseaux sociaux ;
- anticiper les crises en identifiant les sujets et les événements susceptibles d'être "manipulés", en entraînant vos équipes à bien réagir avec des exercices pratiques et en préparant un kit de communication de crise ;
- savoir réagir avec des gestes réflexes simples :
  - vérifier la source des informations et contenus que vous voyez circuler sur vos fils d'actualité ;
  - ne pas se faire le relai des contenus clivants, diffamatoires ;
  - surtout ne pas réagir aux contenus pouvant viser votre entreprise ou administration sous peine d'en augmenter la visibilité.

**Présentation du service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères (VIGINUM) - Grand entretien - IH2EF - Page 7**

Cet entretien est extrait du dossier [Intelligence économique](#).