

Entretien avec Anne-Sophie Dhiver, cheffe de service adjointe de VIGINUM

Concrètement, comment VIGINUM détecte et caractérise les opérations d'ingérence numérique étrangère ciblant la France ?

Pour comprendre le travail de VIGINUM, il faut d'abord se référer à la mission qui lui a été confiée : le rôle du service est de protéger le débat public numérique national contre les ingérences numériques conduites par des acteurs étrangers.

La caractérisation d'une ingérence numérique étrangère répond à une définition précise qui s'appuie sur quatre critères qui doivent être réunis : l'implication d'un acteur étranger, une méthode de diffusion artificielle ou automatisée, massive et délibérée, des contenus manifestement inexacts ou trompeurs et, enfin, une activité susceptible de porter atteinte aux intérêts fondamentaux de la Nation.

Concrètement, VIGINUM s'appuie sur l'analyse de données publiquement accessibles sur les réseaux sociaux, les plateformes numériques et les sites Internet. Nos analystes recherchent des comportements inauthentiques qui peuvent révéler une opération malveillante coordonnée : des réseaux de faux comptes, des sites usurpant l'identité de médias ou d'institutions, des publications automatisées ou encore des mécanismes d'amplification artificielle.

Lorsqu'une opération informationnelle suspecte est identifiée, nos équipes cherchent à reconstituer la manœuvre : ses infrastructures numériques, ses modes de diffusion, les acteurs qui y participent et les objectifs qu'elle poursuit.

Cette exigence est fondamentale : VIGINUM n'est pas une entreprise de *fact-checking*, et son rôle n'est pas de dire aux citoyens ce qui est vrai ou faux. Une opinion politique ou polémique, même particulièrement virulente, ne constitue évidemment pas une ingérence étrangère. Notre travail porte sur les procédés de manipulation, pas sur les opinions exprimées.

Nous faisons aujourd'hui face à une menace persistante et massive. En 2025, VIGINUM a détecté 432 opérations d'ingérence numérique étrangère. À la mi-juillet 2026, nous en avons déjà détecté 430.

Ces opérations peuvent être conduites par des acteurs étatiques, mais également par des prestataires privés ou des opérateurs motivés par des intérêts économiques. Les modes opératoires *Storm-1516* ou *Rokh Solis*, actifs lors de la campagne des élections municipales de 2026, illustrent notamment la sophistication croissante de ces dispositifs, qui combinent faux sites Internet, réseaux de comptes inauthentiques et usages détournés de l'intelligence artificielle.

Notre rôle consiste enfin à transformer cette connaissance technique en capacité d'action. Les analyses de VIGINUM alimentent la réponse interministérielle et peuvent donner lieu à des publications publiques destinées à révéler les méthodes employées.

Face à cette menace, l'action de réponse que mène VIGINUM, en lien étroit avec ses partenaires interministériels et les administrations compétentes, s'applique à trois niveaux. Le premier consiste à agir sur les auteurs de ces opérations, en leur imposant un coût opérationnel et diplomatique, notamment par la dénonciation publique de leurs manœuvres et la mobilisation de régimes de sanctions. Le deuxième vise à responsabiliser les plateformes numériques qui hébergent notre débat public, en lien avec l'ARCOM et l'Union européenne, afin de limiter l'exploitation de leurs services à des fins de manipulation. Enfin, le

troisième consiste à agir auprès des citoyens, premières cibles de ces opérations, en renforçant la résilience informationnelle de la société, qui constitue le rempart le plus efficace et le plus durable face à une menace devenue permanente et omniprésente.

Quels sont les défis auxquels VIGINUM est confronté ?

Nous faisons aujourd'hui face à une menace qui a profondément changé de nature. Elle est devenue permanente, massive et protéiforme. Pour comprendre les difficultés auxquelles nous sommes confrontés, je distinguerais trois grands facteurs de pression qui se cumulent et se renforcent mutuellement.

Le premier est d'ordre **stratégique** : les ingérences informationnelles sont devenues un instrument à part entière des stratégies de déstabilisation de certaines puissances étrangères.

Nous observons des acteurs qui se sont durablement prépositionnés dans notre débat public numérique. Ils disposent d'infrastructures complexes, de réseaux de faux comptes et parfois de prestataires privés qui leur permettent de conduire des opérations dans la durée, mais aussi de réagir très rapidement à l'actualité.

Leurs objectifs peuvent être différents. Certains cherchent à semer le chaos, à exacerber les divisions et à affaiblir la confiance des citoyens dans les institutions. D'autres cherchent à promouvoir leur modèle politique ou à instrumentaliser des revendications existantes pour servir leurs intérêts stratégiques.

Le deuxième facteur de pression est **systémique** : il tient au fonctionnement même de l'écosystème numérique et au modèle économique des grandes plateformes.

Les ingérences numériques étrangères prospèrent dans un environnement où la visibilité d'un contenu dépend largement de sa capacité à susciter des interactions, davantage que de sa fiabilité. Cette logique favorise les contenus spectaculaires, polarisants ou trompeurs, que les acteurs malveillants savent exploiter.

Nous assistons ainsi à l'émergence d'une véritable économie de la manipulation de l'information. De nouveaux opérateurs, notamment en Asie du Sud-Est ou en Afrique de l'Ouest, produisent massivement des contenus destinés aux audiences françaises, non pas nécessairement pour servir les intérêts d'un État, mais pour générer des revenus publicitaires.

Cette évolution constitue un défi majeur, car la menace ne dépend plus uniquement de la volonté d'acteurs étatiques : elle est aussi alimentée par les incitations économiques de l'écosystème numérique.

La réponse doit donc être également réglementaire, en particulier à l'échelle européenne, afin de responsabiliser les plateformes, de renforcer la transparence de leurs algorithmes et de limiter la rentabilité des comportements inauthentiques.

Le troisième facteur de pression est **technologique** : l'intelligence artificielle provoque un changement d'échelle dans la production et la diffusion des manipulations de l'information.

L'IA permet aujourd'hui de produire à très faible coût des textes, des images, des vidéos ou des voix synthétiques particulièrement crédibles. Elle facilite également l'automatisation des campagnes et leur adaptation à différentes audiences.

Elle ouvre enfin de nouveaux vecteurs de manipulation, notamment à travers les agents conversationnels et les risques d'empoisonnement des modèles de langage.

Cette évolution accentue une asymétrie fondamentale : il est devenu extrêmement facile et peu coûteux de fabriquer des contenus trompeurs, alors que leur détection et leur vérification nécessitent toujours du temps, des compétences et des moyens.

Le défi pour VIGINUM est donc de maintenir ses capacités technologiques à l'état de l'art, mais aussi de tirer parti des possibilités offertes par l'intelligence artificielle pour améliorer la détection des opérations.

Face à une menace informationnelle persistante et omniprésente, comment renforcer la résilience de la société face à ces opérations ?

Face à une menace devenue permanente et massive, la réponse ne peut pas être uniquement opérationnelle ou technologique. Elle doit aussi reposer sur le renforcement de la résilience de notre société.

C'est pourquoi la [stratégie nationale de lutte contre les manipulations de l'information](#), publiée en février 2026, fait de la résilience de la Nation une priorité. Cette ambition repose sur trois leviers complémentaires.

Le premier est l'éducation aux médias et à l'information. Il s'agit de donner aux citoyens, et en particulier aux plus jeunes, les moyens d'exercer leur esprit critique, de vérifier leurs sources et de comprendre les mécanismes de manipulation. Cette éducation doit être transgénérationnelle. Elle commence à l'école, mais concerne également les acteurs publics, privés et associatifs. [L'Académie de la lutte contre les manipulations de l'information](#) inaugurée en septembre 2026 au sein de VIGINUM contribue à structurer cette filière et à rapprocher la recherche, l'administration et la société civile.

Le deuxième est la transparence sur la menace. En publiant ses rapports et ses analyses, VIGINUM contribue à rendre visibles les méthodes employées par les acteurs malveillants et permet à chacun de mieux reconnaître ces opérations. L'objectif est de transformer notre connaissance opérationnelle de la menace en un bien commun.

Enfin, le troisième est la responsabilisation des plateformes numériques. Leurs systèmes de recommandation et leurs marchés publicitaires organisent une part majeure de l'accès à l'information. La résilience suppose davantage de transparence sur le fonctionnement des algorithmes, sur les publicités, sur les contenus synthétiques et les réseaux coordonnés, ainsi qu'un meilleur accès aux données pour les chercheurs. Elle exige aussi d'agir sur l'économie de la désinformation : tant que l'indignation, le mensonge et l'inauthenticité restent profitables, de nouveaux opérateurs apparaîtront.

La résilience ne signifie pas rendre la société imperméable à toute influence : une telle société serait une société fermée. L'ambition démocratique est de rester ouverte sans être désarmée, pluraliste sans être manipulable et ferme sans renoncer à l'État de droit.