Guerre informationnelle et vulnérabilité des acteurs économiques : cartographie d'une menace hybride

Document réalisé par Athénaïs JALABERT DOURY

Pourquoi l'entreprise est-elle devenue une cible ?

Jusqu'au milieu des années 2020, la lutte contre les manipulations de l'information (LMI) restait perçue comme une affaire d'État : élections, diplomatie, défense. Le guide conjoint publié en décembre 2025 par VIGINUM et le CDSE (Cercle des Directeurs de Sécurité des Entreprises) acte un basculement de doctrine.

Trois constats structurent ce basculement. D'abord, **la notoriété attire le risque** : plus un dispositif, une marque ou un événement est visible, plus il devient un support de narratifs prêts à l'emploi pour des acteurs hostiles ; le cas des Jeux olympiques et paralympiques de Paris 2024 illustre ce mécanisme à grande échelle. Ensuite, **le risque se propage par ricochet dans l'écosystème** : sous-traitants, sponsors, prestataires de transport, de sécurité ou d'événementiel peuvent être atteints indirectement, sans être eux-mêmes la cible initiale. Enfin, **le faux peut précéder le vrai** : un contenu trompeur, même réfuté ensuite, peut structurer durablement une perception ; la réfutation n'efface pas l'empreinte cognitive de la première exposition.

Les chiffres confirment l'accélération. VIGINUM a recensé 230 phénomènes inauthentiques de manipulation de l'information en 2023, soit une hausse de près de 40 % par rapport à 2022 ; ce total était déjà dépassé au 1er octobre 2024, porté par des dispositifs informationnels « particulièrement persistants » et « très opportunistes », selon les mots de Marc-Antoine Brillant, chef de VIGINUM, devant la commission des affaires étrangères du Sénat. En juin 2026, ce responsable constatait publiquement que « les entreprises n'ont pas assez pris conscience de l'impact des menaces informationnelles » et appelait à sensibiliser en priorité les comités de direction

Typologie de menaces informationnelles visant l'entreprise

Ingérence numérique étrangère à effet de ricochet économique	Une opération conçue pour un objectif géopolitique (déstabilisation d'un État, érosion de la confiance institutionnelle) qui instrumentalise une entreprise, souvent une institution financière ou un opérateur stratégique, comme vecteur ou comme cible secondaire.
Fraude par IA générative et usurpation d'autorité interne	*Deepfakes* audio et vidéo imitant un dirigeant, un directeur financier ou un collègue, déployés en temps réel lors d'appels visio ou d'échanges vocaux pour contourner les procédures de validation financière.
Panique informationnelle authentique amplifiée	Contagion virale d'une inquiétude réelle (fragilité financière, défaut qualité, incident) via les réseaux sociaux, qui accélère et amplifie une crise au point de la rendre auto-réalisatrice sans qu'aucun contenu ne soit nécessairement faux.
Privatisation et commercialisation de la guerre informationnelle	Apparition d'officines privées proposant des prestations de déstabilisation informationnelle « clés en main » (faux sites, comptes inauthentiques, publicités calomnieuses) à des clients étatiques ou non étatiques, brouillant la frontière entre ingérence d'État et concurrence déloyale entre organisations.
Dénigrement thématique, usurpation de marque et boycotts informationnels	Campagnes ciblant la réputation d'une marque sur des sujets sensibles (environnement, droits sociaux, positionnement géopolitique), mêlant griefs réels, exagérations et contenus fabriqués, avec un objectif d'érosion de la confiance consommateur plutôt que de fraude financière directe.

CARTOGRAPHIE DE L'ÉCOSYSTÈME : QUI AGIT, QUI RÉGULE, QUI DÉFEND ?

→ ÉTATIQUE / DÉFENSIF

VIGINUM (créé par décret le 13 juillet 2021, rattaché au SGDSN) détecte et caractérise les ingérences numériques étrangères avec une vingtaine d'analystes spécialisés en sources ouvertes (OSINT) ; il a ouvert en février 2025, lors du Sommet pour l'action sur l'IA à Paris, sa bibliothèque logicielle D3lta en licence libre. L'ANSSI couvre le volet cyber et accompagne l'extension de NIS2, qui fera passer de 500 à 15 000 le nombre d'entités françaises soumises à des obligations de sécurité.

→ RÉGULATEUR SUPRANATIONAL (Commission européenne)

Le Code de conduite sur la désinformation, initié en 2018 et renforcé en 2022, a été intégré au Digital Services Act le 13 février 2025 et est devenu pleinement opposable le 1er juillet 2025 pour les très grandes plateformes (VLOP/VLOSE) : Meta, Google, TikTok, Microsoft notamment.

→ ÉTATIQUE / OFFENSIF IDENTIFIÉ

Doppelgänger/RRN, Matriochka et Portal Kombat (écosystème pro-russe), réseau « Spamouflage » (Chine), Baku Initiative Group (Azerbaïdjan) figurent parmi les dispositifs documentés publiquement par VIGINUM entre 2023 et 2025 comme ciblant l'espace informationnel français.

→ PRIVÉ / MERCENAIRE

Officines d'influence « as a service » – La société BlackCore, qui se décrivait comme une entreprise « d'influence, de cyber et de technologie conçue pour l'ère moderne de la guerre de l'information », illustre l'émergence d'un marché privé de la déstabilisation informationnelle, accessible à des commanditaires non étatiques.

→ SOCIÉTÉ CIVILE ET VÉRIFICATION

Les cellules de fact-checking (AFP notamment), l'Observatoire européen des médias numériques (EDMO) et le CDSE, qui réunit les directeurs de sécurité des grandes entreprises françaises, forment le maillage de vérification et de doctrine partagée avec l'État.

→ INTERNE À L'ENTREPRISE

La gouvernance interne reste le maillon décisif : direction de la sécurité, direction de la communication, RSSI, direction juridique et comité exécutif doivent partager une même grille de lecture du risque informationnel, ce que le guide VIGINUM-CDSE désigne comme une « transformation culturelle ».

Point de vigilance : l'autorégulation des plateformes recule au moment précis où la menace progresse. Selon une analyse de Democracy Reporting International, les engagements pris par les plateformes au titre du Code de conduite ont diminué de 31 % entre 2022 et 2025, avec un repli de 64 % sur les seules mesures de soutien aux fact-checkers, X ayant quitté intégralement le dispositif dès 2023.

LA CHAÎNE DE TRAITEMENT DE LA MENACE INFORMATIONNELLE

6 phases, du signal faible à la résilience installée, une chaîne désormais hybridée avec celle de la gestion de crise cyber, conformément à la doctrine portée par le guide VIGINUM-CDSE.

1) Veille et détection
Surveillance continue des signaux faibles : mentions de marque, usurpations, comptes inauthentiques, pics de viralité anormaux, dérives narratives autour d'un événement exposé (lancement de produit, AG, controverse sectorielle). Repose sur le social listening, l'OSINT et des outils de détection de l'inauthenticité (classification de bots par réseau de following/followers, analyse de coordination).
Outils de référence : bibliothèque D3lta (VIGINUM, open source depuis 2025), classificateurs de comptes automatisés, cellules de veille internes reliées au CDSE.

2) Qualification et caractérisation
Distinguer une critique légitime d'une manœuvre inauthentique : critères d'inauthenticité (comptes coordonnés, erreurs de ciblage trahissant une gestion manuelle à distance), d'intentionnalité et de viralité réelle. Important : la caractérisation technique (constater l'inauthenticité) et l'attribution politique (désigner un commanditaire étatique) relèvent de processus distincts → VIGINUM caractérise, l'attribution politique appartient au ministère des Affaires étrangères, en coordination interministérielle.

3) Décision et déclenchement de la gouvernance de crise
Activation d'une cellule de crise hybride associant sécurité, communication, juridique, RSSI et direction générale, sur la base de seuils d'alerte préétablis. C'est à ce stade qu'est arbitré le risque dit « effet Streisand » : révéler une manœuvre à faible portée peut, paradoxalement, lui donner la visibilité qu'elle n'avait pas.

4) Réponse opérationnelle
Contre-narratif factuel et proportionné, signalement aux plateformes (notices DSA), action en justice si nécessaire (usurpation d'identité, diffamation, ingérence) → vérification systématique par un canal indépendant pour toute instruction financière sensible reçue par audio, vidéo ou messagerie, avant toute exécution.

5) Communication de crise et parties prenantes
Cohérence du discours entre recherche des faits, protection des actifs et défense de l'image : une crise informationnelle sanctionne en priorité les contradictions internes. Séquencement des prises de parole avec salariés, actionnaires, autorités et médias.

6) Retour d'expérience et résilience long terme
Intégration du risque informationnel dans la cartographie globale des risques (ERM), au même rang que le risque cyber. Le guide VIGINUM-CDSE recommande des exercices hybrides : scénarios purement informationnels, scénarios cyber et crises mixtes où un incident technique sert de carburant à une campagne de manipulation, ou inversement → exercice de serious game ou de wargame.

ÉTUDES DE CAS DOCUMENTÉES

1 Matriochka, l'usurpation visant à provoquer une panique bancaire

Active depuis au moins septembre 2023 et documentée par VIGINUM dans un rapport public du 10 juin 2024, la campagne « Matriochka » diffuse de faux contenus usurpant l'identité de médias français (Le Parisien, Le Monde, Le Figaro, France 24) sur des canaux Telegram russophones, puis les fait relayer sur X par des comptes inauthentiques qui interpellent directement les rédactions pour leur demander d'en vérifier l'authenticité. Cette mécanique démultiplie artificiellement la portée du contenu.

Le 7 février 2024, une vidéo usurpant l'organisation étudiante GUD menace de « brûler la Banque de France », accusée de mentir sur sa solvabilité, en lien avec une usurpation de la DGSI. L'objectif assumé est d'inciter la population à un retrait massif de liquidités. VIGINUM qualifie la manœuvre d'ingérence numérique étrangère susceptible de porter atteinte aux intérêts fondamentaux de la Nation.

ENSEIGNEMENT → Les institutions financières demeurent des cibles privilégiées de la déstabilisation à visée systémique : l'usurpation de marque et d'autorité (médias, services de renseignement) y est utilisée comme accélérateur de panique, bien au-delà du cas individuel.

2 Silicon Valley Bank, quand la vérité devient virale plus vite que la réponse

Le 9 mars 2023, les volumes de tweets mentionnant le ticker boursier « SIVB » bondissent près de deux heures et demie avant que la conversation grand public ne s'empare du sujet « SVB ». Une étude académique menée a posteriori établit une corrélation statistique entre l'intensité des échanges sur Twitter et les pertes boursières horaires de la banque, avec un effet de contagion mesurable vers d'autres établissements régionaux fragiles, dont First Republic. Il ne s'agit pas, ici, de désinformation orchestrée, mais de l'amplification virale d'une inquiétude fondée : la communication interpersonnelle entre déposants, largement composés d'entrepreneurs technologiques hyperconnectés, a transformé une fragilité financière réelle en bank run en quelques heures.

ENSEIGNEMENT → La résilience informationnelle ne concerne pas que le faux : une organisation peut être emportée par la vitesse de circulation d'une information vraie qu'elle n'a pas su contextualiser ni devancer durant la fameuse « golden hour » de la gestion de crise.

3 BlackCore, la guerre informationnelle vendue comme un service

À la veille des élections municipales françaises de mars 2026, trois candidats de La France insoumise (à Marseille, Toulouse et Roubaix) sont visés par une campagne de dénigrement : faux sites accusant l'un d'eux de violences sexuelles, comptes coordonnés et publicités dénigrantes dans la presse locale. VIGINUM révèle une opération d'ingérence numérique « à portée limitée ». Une enquête conjointe menée par la presse française et israélienne désigne ensuite la société BlackCore, qui se présentait comme une « entreprise d'élite d'influence, de cyber et de technologie conçue pour l'ère moderne de la guerre de l'information ». De son côté, Meta retire un réseau de comptes coordonnés originaire d'Israël.

VIGINUM indique que ce mode opératoire a également été repéré en marge d'élections en Écosse, à New York, en Angola et au Togo. Le parquet de Paris ouvre une enquête. Le site et la page LinkedIn de BlackCore disparaissent après l'exposition médiatique ; l'identité du ou des commanditaires reste, à ce stade, non établie.

ENSEIGNEMENT → Ce dossier déplace le centre de gravité de la menace : des capacités auparavant réservées à des services étatiques deviennent un service commercial achetable par un concurrent, un activiste organisé ou toute partie prenante hostile à une entreprise, indépendamment de tout enjeu géopolitique.

Le guide VIGINUM-CDSE, la première doctrine partagée État-entreprises

Publié en décembre 2025, ce guide constitue le premier texte coécrit par un service de l'État et le monde économique français sur ce sujet. Il s'appuie notamment sur le retour d'expérience des Jeux olympiques et paralympiques de Paris 2024, au cours desquels deux dynamiques opposées ont été observées : d'une part, un volume massif de contenus négatifs issus de la mouvance « MAGA » américaine, sans effet mesurable sur une opinion publique largement conquise par l'événement sportif ; d'autre part, des contenus diffusés par l'Azerbaïdjan en bien plus faible quantité, mais qui ont effectivement atteint et mobilisé des communautés calédoniennes favorables à l'indépendance. Ce constat démontre que le volume d'une campagne n'est pas corrélé à son impact réel.

ENSEIGNEMENT → Mesurer une menace informationnelle exige une grille d'analyse fine de l'audience et du contexte culturel ciblés, et non un simple comptage des publications : un principe directement transposable à la veille de marque en entreprise.

ENSEIGNEMENTS TRANSVERSAUX

- **Le volume n'est pas l'impact** : une campagne massive mais hors-sol (mouvance MAGA aux JOP 2024) peut produire moins d'effets qu'une campagne discrète mais culturellement ciblée (Azerbaïdjan / Nouvelle-Calédonie).
- **Le faux structure la perception avant même d'être démenti** : la réfutation n'efface pas la première impression, la vitesse de détection compte autant que la qualité de la réponse.
- **Le facteur humain reste le maillon décisif** : seule la réaction humaine qui est le réflexe de vérification indépendante peut faire diverger l'issue, qu'importe le mode opératoire.
- **L'effet Streisand doit être arbitré et non ignoré** : révéler une manœuvre à faible portée peut, paradoxalement, lui offrir la visibilité qu'elle n'avait pas encore obtenue.
- **La frontière cyber / informationnel s'efface** : un incident technique peut nourrir une campagne de manipulation, et inversement, d'où la doctrine d'exercices hybrides portée par VIGINUM-CDSE.
- **La privatisation des capacités d'influence démocratise la menace** : le précédent BlackCore montre que des moyens auparavant réservés à des services de renseignement deviennent accessibles sur un marché privé.
- **L'autorégulation des plateformes recule quand le risque augmente** : le repli de 31 % des engagements de la plateforme européenne entre 2022 et 2025 transfère mécaniquement davantage de responsabilité de détection vers l'entreprise elle-même.

PERSPECTIVES

Trois dynamiques structurent la suite pour les entreprises : l'accélération de l'IA générative, qui amplifie les volumes de contenus (sans avoir, à ce jour, résolu la massification multilingue de l'astroturfing, selon VIGINUM) ; l'élargissement du périmètre réglementaire, avec NIS2 portant à 15 000 le nombre d'entités françaises couvertes et le futur Bouclier européen pour la démocratie ; enfin, une contrainte budgétaire qui pèse également sur les services de l'État : VIGINUM opère en 2025 dans le cadre d'un budget de 307,6 millions d'euros pour l'ensemble interministériel SGDSN, en repli de 8 millions d'euros par rapport à 2024.

→ **Élever le risque informationnel au rang du risque cyber dans la cartographie ERM** : le comité exécutif doit disposer d'indicateurs de veille informationnelle au même titre que des indicateurs de cybersécurité, et non comme une annexe de la communication.

→ **Installer une cellule de veille permanente reliée à la cellule de crise** : détection des signaux faibles, classification de l'inauthenticité, lien direct avec les responsables communication, juridique et sécurité.

→ **Imposer un canal de vérification indépendant pour toute instruction financière sensible** : leçon directe du cas Arup : aucune validation de virement ne doit reposer uniquement sur un appel, un message vocal ou une visioconférence, sans rappel à un numéro préalablement connu.

→ **Organiser des exercices hybrides cyber + informationnel** : conformément à la doctrine VIGINUM-CDSE => scénarios purs, scénarios mixtes, avec implication du comité de direction et non des seules équipes opérationnelles.

→ **Cartographier les dépendances de l'écosystème** : sous-traitants, sponsors, prestataires événementiels et logistiques peuvent être atteints par ricochet -> leur exposition doit être intégrée à l'analyse de risque de l'entreprise elle-même.

→ **Formaliser les canaux de signalement et de coopération externe** : procédures de notice auprès des plateformes au titre du DSA, lien identifié avec VIGINUM, l'ANSSI et le CDSE pour les organisations éligibles.

→ **Exercer une due diligence sur la privatisation de l'influence** : surveiller l'émergence d'officines « as a service » et intégrer ce risque dans l'analyse de la concurrence déloyale et de l'intelligence économique, à l'image de l'épisode avec BlackCore.