Institut EGA

# Policy paper

## La désinformation comme risque stratégique d'entreprise

Athénaïs Jalabert
Directrice du département Lutte informationnelle et influence de l'Institut d'études de géopolitique appliquée (Iega)

22.06.26

# SOMMAIRE

# Résumé exécutif

Indépendamment de leur taille ou de leur secteur d'activité, les entreprises sont désormais exposées à une menace informationnelle dont les conséquences économiques, réputationnelles et opérationnelles ne cessent de croître. À cet égard, Sopra Steria, acteur majeur du secteur technologique européen, souligne dans son étude consacrée à la désinformation et à son impact économique que le coût global de la désinformation pour l'économie mondiale a atteint 417 milliards de dollars en 2024.

Ce montant se décompose notamment en :

- 393 milliards de dollars de pertes financières directes ;
- 227 milliards de dollars de dépenses de consommation influencées par de faux avis en ligne ;
- 11 milliards de dollars de coûts associés aux deepfakes et aux fraudes reposant sur l'intelligence artificielle ;
- 5,5 milliards de dollars de pertes liées aux escroqueries cryptographiques de type pig butchering.

Cette dynamique est d'autant plus préoccupante que le Forum économique mondial classe la désinformation parmi les principaux risques systémiques mondiaux depuis 2023. L'essor des capacités offertes par l'intelligence artificielle générative, la sophistication croissante des contenus synthétiques et l'utilisation de vecteurs numériques à très large échelle renforcent considérablement le potentiel de nuisance des acteurs malveillants, qu'ils soient étatiques, paraétatiques ou criminels.

Face à cette évolution du paysage des menaces, **les organisations demeurent insuffisamment préparées**. En 2022, seules 25 % d'entre elles disposaient d'un dispositif de prévention et de mitigation jugé efficace face aux risques combinés de cyberattaques et de campagnes de désinformation, révélant un déficit persistant de résilience informationnelle au sein du tissu économique mondial.

Dans ce contexte, le présent policy paper vise à analyser les principales formes de désinformation ciblant les entreprises, à examiner plusieurs cas emblématiques observés en Europe et aux États-Unis, ainsi qu'à évaluer les stratégies de gestion des risques et les mécanismes de résilience mis en œuvre par les organisations afin de renforcer leur capacité de défense face à ces menaces hybrides.

# Définition et cadre conceptuel

L'analyse des menaces informationnelles pesant sur les entreprises nécessite, en préalable, de distinguer trois catégories conceptuelles souvent amalgamées dans le débat public :

- la mésinformation,
- la désinformation et,
- la malinformation.

Ces trois catégories constituent les principaux registres de manipulation informationnelle auxquels les organisations sont confrontées. Dans la pratique, les campagnes les plus sophistiquées combinent fréquemment des éléments de mésinformation, de désinformation et de malinformation afin de maximiser leur portée, leur crédibilité et leur impact sur la cible visée.

Bien que distinctes par leur nature et leurs finalités, ces trois formes de manipulation de l'information peuvent être mobilisées simultanément au sein d'une même campagne d'influence ou d'atteinte à la réputation.

### 1. La mésinformation (misinformation)

La mésinformation désigne la **diffusion d'informations fausses, erronées ou trompeuses sans intention délibérée de nuire**. Elle résulte généralement d'erreurs de bonne foi, d'interprétations inexactes, de rumeurs non vérifiées ou encore de phénomènes de viralité propres aux environnements numériques.

Dans le contexte des entreprises, la mésinformation peut se traduire par la **circulation involontaire d'informations inexactes concernant un produit, un service ou une décision stratégique**, sans que les personnes relayant ces contenus ne cherchent délibérément à porter préjudice à l'organisation concernée.

*Exemple* : un consommateur partage sur les réseaux sociaux une information erronée relative à la composition ou à la sécurité d'un produit, contribuant involontairement à alimenter une perception négative de l'entreprise.

### 2. La désinformation (disinformation)

La désinformation renvoie à la **production et à la diffusion intentionnelles d'informations fausses ou manipulées dans le but de tromper, d'influencer ou de nuire à une cible identifiée**. Elle implique généralement l'existence d'un acteur, d'un objectif stratégique, de méthodes spécifiques et de vecteurs de diffusion soigneusement sélectionnés.

Dans l'environnement économique contemporain, les campagnes de désinformation peuvent viser à **déstabiliser** une entreprise, à **altérer sa réputation**, à **influencer les comportements des consommateurs** ou encore à **affecter sa valorisation financière**.

*Exemple* : la diffusion coordonnée d'un faux communiqué de presse annonçant des difficultés financières ou des irrégularités majeures au sein d'une entreprise cotée, dans le but de provoquer une chute de son cours boursier.

### 3. La malinformation (malinformation)

La malinformation se distingue des deux catégories précédentes en ce qu'elle repose sur l'**utilisation d'informations authentiques, mais exploitées de manière malveillante**. Les contenus concernés peuvent être sortis de leur contexte, présentés de façon sélective ou instrumentalisés afin de produire un effet de nuisance disproportionné.

Cette forme d'attaque est particulièrement difficile à contrer, dans la mesure où **elle s'appuie sur des éléments factuellement exacts tout en en déformant le sens ou la portée**.

*Exemple* : la divulgation ciblée d'un courrier électronique interne ou privé d'un dirigeant, extrait de son contexte initial afin d'alimenter une campagne de discrédit ou de fragiliser la réputation de l'entreprise.

# Typologie des attaques informationnelles ciblant les entreprises

## Une classification des principales menaces informationnelles

Les attaques informationnelles dirigées contre les entreprises se sont diversifiées au cours de la dernière décennie sous l’effet de la transformation numérique, de l’interconnexion des marchés et de l’émergence de nouvelles technologies de manipulation de l’information. Elles poursuivent des objectifs variés — financiers, concurrentiels, idéologiques ou géopolitiques — et mobilisent des modes opératoires de plus en plus sophistiqués.

**Six grandes catégories de menaces peuvent être distinguées.**

### *1. Manipulation financière et boursière*

Cette catégorie regroupe les opérations visant à influencer la valorisation d’une entreprise ou le comportement des investisseurs par la diffusion d’informations financières fausses ou trompeuses. Les vecteurs utilisés incluent notamment les faux communiqués de presse, les rumeurs d’irrégularités comptables, les allégations de fraude ou encore les annonces fictives de fusion-acquisition.

Ces attaques ciblent principalement les entreprises cotées, dont la sensibilité aux flux informationnels est particulièrement élevée. L’objectif consiste généralement à provoquer des variations de cours exploitables à des fins spéculatives ou à déstabiliser durablement une entreprise concurrente.

**Étude de cas : l'affaire Vinci (2016)**

**Contexte**. Le 22 novembre 2016, un faux communiqué de presse attribué à Vinci SA est transmis à plusieurs médias financiers internationaux, dont Bloomberg. Les auteurs de l'opération ont usurpé l'identité du groupe en créant une adresse électronique imitant celle de son service de communication. Le document annonçait prétendument la découverte d'irrégularités comptables majeures dissimulant 3,5 milliards d'euros de pertes ainsi que le licenciement du directeur financier. L'information est alors relayée par Bloomberg avant d'être intégrée aux systèmes de traitement automatisé utilisés par de nombreux acteurs financiers.

**Impact**. En quelques minutes, l'action Vinci perd plus de 18 % de sa valeur avant de remonter partiellement après le démenti officiel du groupe. L'épisode conduit l'Autorité des marchés financiers (AMF) à ouvrir une enquête. En 2019, Bloomberg est sanctionné à hauteur de cinq millions d'euros pour manquements aux obligations de vérification, décision confirmée en cassation en 2024.

**Réponse de l'entreprise**. Vinci procède à un démenti immédiat via ses canaux institutionnels et engage des actions judiciaires en coopération avec les autorités de régulation.

**Enseignements**. Ce cas met en évidence la nécessité de renforcer les procédures de vérification des informations financières à fort impact avant leur diffusion. Il souligne également l'importance, pour les entreprises cotées, de sécuriser leur identité numérique, notamment par la protection des domaines internet et des systèmes d'authentification des courriels. Enfin, il démontre que la rapidité de réaction demeure un facteur déterminant dans la limitation des dommages financiers et réputationnels.

### *2. Usurpation d'identité institutionnelle ou dirigeante*

Cette catégorie regroupe l'ensemble des opérations consistant à se faire passer pour une organisation ou l'un de ses représentants afin de tromper des tiers. Les techniques employées comprennent les faux communiqués de presse, les faux profils sur les réseaux sociaux, le clonage de sites institutionnels ainsi que, de plus en plus fréquemment, l'utilisation de contenus synthétiques générés par intelligence artificielle.

Ces attaques visent principalement les investisseurs, les partenaires commerciaux, les journalistes ou les collaborateurs de l'entreprise concernée.

**Étude de cas : WPP (2024)**

L'incident ayant visé WPP illustre le degré de sophistication atteint par les opérations d'usurpation à l'ère de l'intelligence artificielle générative.

**Contexte**. En mai 2024, des fraudeurs tentent d'usurper l'identité de Mark Read, directeur général du groupe, afin d'obtenir des transferts financiers et des informations sensibles. L'opération combine plusieurs techniques : création d'un faux compte WhatsApp utilisant la photographie publique du dirigeant, organisation d'une réunion sur Microsoft Teams intégrant des extraits vidéo du PDG et recours à un clone vocal généré par intelligence artificielle. Les attaquants demandent à une filiale du groupe de créer une nouvelle entité juridique et d'effectuer des opérations financières au profit des fraudeurs.

**Impact**. Grâce à la vigilance des collaborateurs ciblés, aucune perte financière n'est enregistrée.

**Réponse de l'entreprise**. La direction diffuse rapidement une alerte interne détaillant les indicateurs de compromission observés. WPP publie également une mise en garde officielle et coopère avec les autorités compétentes.

**Enseignements**. Cette affaire démontre l'importance croissante des mécanismes de vérification indépendants (out-of-band verification) pour toute demande impliquant des flux financiers ou des données sensibles. Elle souligne également la nécessité de former les collaborateurs aux risques associés aux deepfakes et à l'ingénierie sociale augmentée par l'intelligence artificielle.

### *3. Campagnes de dénigrement coordonnées*

Les campagnes de dénigrement coordonnées reposent sur la diffusion massive et organisée de contenus négatifs visant une entreprise, une marque, un produit ou un dirigeant. Elles s'appuient fréquemment sur des réseaux de comptes automatisés (bots), des fermes à clics ou des communautés militantes organisées.

L'objectif consiste à saturer l'espace informationnel afin de façonner une perception négative durable auprès du grand public, des investisseurs ou des autorités publiques. Les motivations peuvent être concurrentielles, idéologiques, activistes ou géopolitiques.

Ces opérations sont particulièrement efficaces lorsqu'elles exploitent des controverses existantes ou des vulnérabilités réputationnelles préexistantes.

***4. Diffusion de rumeurs relatives à la sécurité des produits et services***

Cette catégorie regroupe les campagnes visant à remettre en cause la sécurité, la qualité ou la conformité d'un produit ou d'un service par la diffusion d'informations fausses ou décontextualisées.

Les allégations peuvent porter sur de prétendus risques sanitaires, des défauts techniques, des contaminations, des failles de sécurité ou des pratiques de fabrication supposément contraires aux normes en vigueur.

Les secteurs agroalimentaire, pharmaceutique, cosmétique, chimique et automobile sont particulièrement exposés à ce type de menace, dans la mesure où la confiance des consommateurs constitue un actif stratégique essentiel.

***5. Manipulation de la chaîne d'approvisionnement et de l'écosystème de partenaires***

Les entreprises ne sont plus uniquement ciblées en tant qu'entités isolées, mais également à travers leur écosystème économique. Cette catégorie d'attaques vise à fragiliser les relations de confiance entre une entreprise et ses fournisseurs, sous-traitants, distributeurs ou partenaires institutionnels.

Les campagnes peuvent prendre la forme de fausses informations relatives à la solvabilité d'un fournisseur, à la conformité réglementaire d'un partenaire ou encore à des pratiques éthiques supposément problématiques.

L'objectif recherché est souvent la rupture de relations contractuelles, la perturbation des chaînes logistiques ou la création d'incertitudes susceptibles d'affecter la continuité des activités.

***6. Manipulation de la marque employeur et des processus de recrutement***

La réputation employeur constitue désormais un levier stratégique de compétitivité. À ce titre, elle représente également une cible privilégiée des opérations informationnelles.

Ces attaques reposent notamment sur la publication coordonnée de faux témoignages d'anciens salariés, la multiplication d'avis négatifs artificiels sur les plateformes d'emploi et de notation professionnelle, ou encore la diffusion de fausses informations relatives aux conditions de travail, à la gouvernance ou à la culture d'entreprise.

Au-delà de leur impact réputationnel immédiat, ces campagnes peuvent affecter durablement la capacité d'une organisation à attirer, recruter et fidéliser les talents dans un contexte de concurrence accrue sur les compétences stratégiques.

L'ensemble de ces catégories illustre l'**élargissement progressif du champ des menaces informationnelles pesant sur les entreprises**.

Longtemps considérées comme des risques essentiellement réputationnels, **ces attaques produisent désormais des effets directs sur la performance économique, la gouvernance, les capacités opérationnelles et la résilience stratégique des organisations**.

Elles constituent ainsi un **enjeu de sécurité économique à part entière**, nécessitant une approche intégrée associant :

- cybersécurité,
- gestion des risques,
- communication de crise et;
- veille informationnelle.

| Type d'attaque | Acteur typique | Canal principal | Cible | Intention | Temporalité |
|---|---|---|---|---|---|
| Manipulation boursière | Acteur financier, vendeur à découvert, concurrent | Médias financiers, fil AFP/Bloomb. | Cours de Bourse, investisseurs | Profit financier | Court terme, précision chirurgicale |
| Faux communiqué | Concurrent, acteur hostile, criminel organisé | Agences de presse, médias | Presse, marchés, partenaires | Déstabilisation profit | Court terme |
| Deepfake dirigeant | Fraudeur, état hostile, concurrent | Visio., messagerie | Collaborateurs banques | Fraude financière | Court terme |
| Dénigrement coordonné | Concurrent, groupe idéologique, hacktiviste | Réseaux sociaux, forums | Opinion publique, consom. | Image, parts de marché | Moyen-long terme |
| Rumeur produit | Concurrent, activiste, état hostile | Réseaux sociaux, forums santé | Consom., régulateurs | Boycott, rappel produit | Variable |
| Manipulation marque employeur | Concurrent RH, ex-salarié malveillant | Glassdoor, LinkedIn, forums | Candidats, talents | Déstabilisation interne | Long terme |
| Malinformat. par fuite | État, concurrent, lanceur d'alerte instrument. | Médias, Wikileaks-type | Opinion, régulateurs, clients | Discrédit, sanction | Variable |

# Logiques d'acteurs, objectifs et vecteurs de diffusion

La compréhension des menaces informationnelles pesant sur les entreprises suppose d'identifier les acteurs qui les portent, les objectifs qu'ils poursuivent ainsi que les vecteurs mobilisés pour atteindre leurs cibles. Contrairement à une perception souvent réductrice, la désinformation économique ne relève pas d'un acteur unique ou d'une seule logique d'action. Elle constitue un espace de confrontation hybride où se croisent intérêts géopolitiques, motivations financières, activisme idéologique et criminalité organisée.

## CARTOGRAPHIE DES ACTEURS MENAÇANTS

### *1. Les acteurs étatiques et para-étatiques*

Les États et les structures qui leur sont liées constituent aujourd'hui des acteurs majeurs de l'écosystème informationnel. Dans une logique de compétition stratégique, ils peuvent recourir à des campagnes de désinformation afin de fragiliser des entreprises considérées comme stratégiques, de limiter l'influence économique d'un concurrent étranger ou encore d'affaiblir une filière industrielle jugée rivale.

Ces opérations s'inscrivent généralement dans une approche plus large de guerre informationnelle et de sécurité économique, où les entreprises deviennent des cibles indirectes des rivalités géopolitiques contemporaines.

L'opération dite Doppelgänger, documentée par les autorités européennes et par Viginum, illustre cette dynamique. Cette campagne reposait notamment sur la création de faux sites internet reproduisant l'apparence de médias reconnus afin de diffuser des contenus manipulés destinés à influencer les perceptions et à accentuer les divisions au sein des sociétés ciblées. Bien que principalement orientées vers le débat public, ces techniques peuvent également être utilisées contre des acteurs économiques stratégiques.

### *2. Les concurrents directs*

Dans certains secteurs fortement concurrentiels, la désinformation peut être utilisée comme un instrument de compétition économique. Ces pratiques, parfois qualifiées de corporate warfare, visent à dégrader la réputation d'un concurrent, à remettre en cause la qualité de ses produits ou à fragiliser la confiance de ses partenaires commerciaux.

Les campagnes peuvent prendre la forme de rumeurs relatives aux conditions d'approvisionnement, à la conformité réglementaire, à la gouvernance ou à la situation financière d'une entreprise.

L'une des caractéristiques majeures de ces opérations réside dans leur faible traçabilité. Les commanditaires cherchent généralement à masquer leur implication en recourant à des intermédiaires, à des prestataires tiers ou à des réseaux de diffusion indirects, rendant l'attribution particulièrement complexe.

### *3. Les acteurs financiers malveillants*

Les marchés financiers constituent un environnement particulièrement sensible aux manipulations informationnelles. Certains acteurs peuvent chercher à tirer profit de fluctuations artificiellement provoquées par la diffusion de fausses informations ou d'informations délibérément trompeuses.
Les stratégies de manipulation peuvent notamment viser à provoquer une chute du cours d'un actif afin de générer un gain financier, notamment dans le cadre de positions vendeuses à découvert (short selling). D'autres opérations peuvent au contraire chercher à créer artificiellement un engouement autour d'une entreprise ou d'un produit financier.

Si ces pratiques sont strictement encadrées par les régulations financières nationales et internationales, leur détection demeure difficile en raison de la rapidité des échanges numériques et de la multiplicité des acteurs impliqués.

### *4. Les groupes hacktivistes et militants*

Les organisations militantes et les collectifs hacktivistes peuvent également recourir à des campagnes informationnelles contre des entreprises dont ils contestent les pratiques ou les orientations stratégiques.

Ces campagnes s'appuient fréquemment sur des mécanismes de viralisation en ligne, des appels au boycott ou des actions coordonnées visant à détériorer l'image publique de l'organisation ciblée. Elles mobilisent souvent un mélange d'informations véridiques, de contenus sortis de leur contexte et, dans certains cas, d'informations inexactes destinées à renforcer le récit militant.

***5. Les acteurs criminels organisés***

La criminalité organisée investit de plus en plus le champ informationnel en raison de son fort potentiel de rentabilité et du faible coût d'entrée permis par les technologies numériques.

Les groupes criminels exploitent notamment les techniques d'usurpation d'identité, les campagnes de fraude au président, les faux communiqués institutionnels ainsi que les deepfakes audio ou vidéo destinés à contourner les mécanismes traditionnels de confiance.

L'intelligence artificielle générative a considérablement accru les capacités opérationnelles de ces acteurs en réduisant les coûts de production de contenus frauduleux et en améliorant leur crédibilité apparente.

***6. Les acteurs internes***

Enfin, certaines menaces proviennent de l'intérieur même des organisations. Anciens collaborateurs, cadres dirigeants évincés, salariés en conflit avec leur employeur ou individus disposant d'un accès privilégié à l'information peuvent devenir des vecteurs de déstabilisation.

Ces acteurs disposent souvent d'une connaissance fine des processus internes, des vulnérabilités organisationnelles et des dynamiques humaines de l'entreprise. Ils peuvent diffuser des informations authentiques de manière sélective, favoriser des opérations de malinformation ou, dans les cas les plus graves, contribuer à la fabrication de faux éléments destinés à accréditer un récit préjudiciable à l'organisation.

## LES PRINCIPAUX VECTEURS DE DIFFUSION

Les campagnes de désinformation contemporaines reposent rarement sur un canal unique. Elles mobilisent généralement plusieurs vecteurs de diffusion simultanément afin d'augmenter leur portée, leur crédibilité et leur résilience face aux tentatives de correction ou de modération.

- **Les réseaux sociaux**

Les plateformes sociales constituent aujourd'hui les principaux accélérateurs de diffusion des contenus manipulés. Grâce aux mécanismes algorithmiques de recommandation, aux réseaux de comptes automatisés (bots) et aux opérations coordonnées d'amplification, une information trompeuse peut atteindre une audience considérable en quelques heures seulement.

Les plateformes professionnelles telles que LinkedIn sont particulièrement utilisées dans les campagnes ciblant les entreprises, les investisseurs ou les dirigeants.

- **Les médias et agences de presse**

Les agences de presse et les médias économiques représentent des cibles privilégiées pour les opérations visant à obtenir une légitimité apparente. L'injection de faux communiqués ou de documents falsifiés dans les circuits d'information professionnels permet d'accélérer considérablement la diffusion du contenu manipulé et d'en accroître la crédibilité.

Les conséquences sont particulièrement importantes lorsque ces informations sont intégrées dans des systèmes de veille automatisés ou dans des plateformes de trading algorithmique.

- **Les messageries professionnelles**

Les outils de communication collaborative tels que WhatsApp, Microsoft Teams, Slack ou Signal constituent des vecteurs de plus en plus exploités par les acteurs malveillants.

L'émergence des deepfakes audio et vidéo renforce la crédibilité des tentatives d'usurpation réalisées sur ces plateformes, notamment lorsqu'elles visent à obtenir des transferts financiers ou des informations sensibles.

- **Les plateformes d'évaluation et d'avis**

Les plateformes d'avis consommateurs et les sites spécialisés dans l'évaluation des employeurs constituent des espaces particulièrement vulnérables aux opérations de manipulation.

Les campagnes coordonnées de faux avis peuvent affecter simultanément la réputation commerciale d'une entreprise, sa marque employeur et la confiance accordée par ses parties prenantes.

- **Les forums spécialisés et communautés numériques**

Les forums d'investisseurs, les communautés professionnelles en ligne et certaines plateformes de discussion constituent des espaces privilégiés pour la diffusion de rumeurs ciblées. Leur forte spécialisation thématique favorise la circulation rapide d'informations non vérifiées auprès de publics susceptibles d'agir immédiatement sur la base des contenus diffusés.

- **Les sites clonés et l'usurpation de l'identité numérique**

Le clonage de sites internet institutionnels, les techniques de typosquatting ou l'usurpation de noms de domaine constituent des méthodes récurrentes permettant de diffuser de fausses informations sous une apparence légitime.
Ces dispositifs sont souvent utilisés en complément d'autres vecteurs afin de renforcer la crédibilité globale de l'opération.

- **Les canaux de communication internes compromis**

Enfin, la compromission ou l'usurpation de canaux de communication internes représente l'une des formes les plus dangereuses de manipulation informationnelle. Lorsqu'un message semble provenir d'une source interne légitime, sa capacité de persuasion augmente considérablement, réduisant les mécanismes habituels de vigilance des collaborateurs.

Cette évolution témoigne d'une convergence croissante entre les menaces cyber et informationnelles. La désinformation ne doit ainsi plus être appréhendée comme un simple risque réputationnel, mais comme une composante à part entière des stratégies contemporaines d'influence, de coercition économique et de déstabilisation organisationnelle.

# Impacts économiques, réputationnels et opérationnels

Les attaques informationnelles dirigées contre les entreprises ne se limitent plus à une simple atteinte à l'image. Elles produisent désormais des effets mesurables sur la valorisation financière, la confiance des parties prenantes, les opérations courantes et l'exposition juridique des organisations. À mesure que les écosystèmes économiques deviennent plus dépendants de l'information en temps réel, la désinformation s'impose comme un facteur de risque systémique susceptible d'affecter durablement la performance et la résilience des entreprises.

### 1. Impact sur les marchés financiers et la valorisation des entreprises

Les marchés financiers constituent l'un des environnements les plus sensibles aux manipulations informationnelles. La vitesse de circulation des informations, l'automatisation croissante des décisions d'investissement et le recours aux outils de traitement algorithmique renforcent considérablement les effets potentiels des campagnes de désinformation.

L'affaire Vinci de novembre 2016 demeure à cet égard l'un des cas les plus emblématiques observés en Europe. La diffusion d'un faux communiqué de presse annonçant la révision des comptes du groupe, la découverte de prétendues irrégularités comptables dissimulant 3,5 milliards d'euros de pertes ainsi que le licenciement du directeur financier provoqua une chute de plus de 18 % du titre en quelques minutes après sa reprise par plusieurs canaux d'information financière. Bien que le démenti rapide de l'entreprise ait permis un rétablissement partiel du cours, l'épisode a engendré des coûts significatifs en matière de volatilité boursière, de crédibilité institutionnelle et de contentieux juridiques.

Au-delà des entreprises directement ciblées, certaines opérations démontrent la capacité de la désinformation à générer des perturbations plus larges sur les marchés. En mai 2023, la diffusion virale d'une image générée par intelligence artificielle représentant une prétendue explosion à proximité du Pentagone provoqua un mouvement de recul temporaire sur plusieurs indices financiers américains avant que l'information ne soit officiellement démentie. Cet épisode illustre le risque croissant de chocs informationnels systémiques alimentés par les technologies de génération de contenu synthétique.

Le cas de Tesla en 2018 met en lumière une autre forme de vulnérabilité : celle liée à la diffusion d'informations trompeuses par des personnalités disposant d'une influence considérable sur les marchés. Les déclarations publiques d'Elon Musk relatives à un projet de retrait de la cote de Tesla, prétendument soutenu par un financement sécurisé, ont entraîné une hausse significative du cours de l'action avant de conduire à une procédure engagée par la Securities and Exchange Commission (SEC) pour manipulation présumée des marchés financiers. Cet épisode démontre que les risques informationnels ne proviennent pas uniquement d'acteurs externes, mais peuvent également résulter de communications émanant de dirigeants eux-mêmes.

### 2. Impact sur la confiance des consommateurs et l'image de marque

Au-delà des marchés financiers, les campagnes de désinformation affectent directement la relation de confiance entre les entreprises et leurs parties prenantes. Les attaques portant sur la qualité des produits, les pratiques sociales, les engagements environnementaux ou la gouvernance peuvent provoquer des réactions rapides de la part des consommateurs, allant du boycott ponctuel à une remise en cause durable de la réputation de l'organisation.

Les conséquences économiques de ces campagnes sont souvent difficiles à quantifier avec précision. Toutefois, la littérature académique et les analyses de gestion de crise convergent pour souligner que la reconstruction d'une réputation gravement dégradée nécessite généralement plusieurs années d'efforts continus. Une crise réputationnelle majeure peut ainsi produire des effets persistants sur les ventes, la fidélisation des clients, la capacité d'attraction des investisseurs et les relations avec les partenaires institutionnels.

Cette vulnérabilité est renforcée par une tendance plus large à l'érosion de la confiance dans les institutions. Dans de nombreuses démocraties occidentales, la défiance croissante à l'égard des gouvernements, des médias et des organisations économiques crée un environnement favorable à la diffusion de récits alternatifs, parfois dénués de fondement factuel.

Dans ce contexte, les entreprises font face à une véritable asymétrie informationnelle : les contenus négatifs, polémiques ou sensationnalistes bénéficient généralement d'une diffusion plus rapide et d'un niveau d'engagement supérieur à celui des démentis ou des rectifications factuelles. Cette dynamique constitue l'un des principaux défis contemporains de la gestion de la réputation.

### 3. Impact opérationnel : fraude, continuité d'activité et prise de décision

Les attaques informationnelles produisent également des effets opérationnels directs susceptibles d'affecter la continuité des activités et les capacités décisionnelles des organisations. L'essor des technologies de synthèse vocale et audiovisuelle a considérablement accru le risque de fraude fondée sur l'usurpation d'identité. Les deepfakes de dirigeants permettent désormais de reproduire avec un haut degré de réalisme l'apparence, la voix et les comportements d'une personne cible afin de convaincre des collaborateurs de réaliser des opérations sensibles.

L'incident survenu à Hong Kong en 2024 illustre cette évolution. À l'issue d'une visioconférence impliquant plusieurs participants artificiellement générés, des employés ont été amenés à effectuer des transferts financiers frauduleux représentant plusieurs dizaines de millions de dollars. Ce type d'attaque démontre que les mécanismes traditionnels de confiance fondés sur la reconnaissance visuelle ou vocale ne constituent plus des garanties suffisantes dans un environnement marqué par l'émergence des contenus synthétiques.

Au-delà des pertes financières immédiates, ces opérations peuvent également perturber les processus de gouvernance, ralentir la prise de décision, mobiliser d'importantes ressources internes de vérification et dégrader durablement le climat de confiance au sein de l'organisation.

**4. mpacts juridiques, réglementaires et de conformité**

Les conséquences des campagnes de désinformation dépassent fréquemment le seul cadre économique ou réputationnel. Une entreprise visée peut également être confrontée à des risques juridiques significatifs, même lorsque les accusations portées à son encontre sont infondées.

La diffusion de fausses allégations peut notamment conduire à l'ouverture d'enquêtes administratives ou réglementaires, à la suspension temporaire de certaines activités, à des litiges commerciaux ou à des contentieux engagés par des investisseurs estimant avoir subi un préjudice économique.

Les entreprises doivent alors consacrer des ressources importantes à la gestion de la crise, à la production d'éléments de preuve et à la restauration de leur crédibilité auprès des autorités compétentes.

Parallèlement, le renforcement des cadres réglementaires visant à lutter contre les manipulations informationnelles modifie progressivement l'environnement de conformité des acteurs privés. En Europe, le Digital Services Act (DSA) impose notamment de nouvelles obligations aux grandes plateformes numériques en matière de gestion des risques systémiques et de diffusion de contenus illicites ou manipulés.

Toutefois, ces évolutions réglementaires ne dispensent pas les entreprises de développer leurs propres capacités de détection, de réponse et de résilience. La responsabilité de la protection de leur réputation, de leurs actifs informationnels et de leurs parties prenantes demeure en grande partie de leur ressort.

L'ensemble de ces éléments confirme que **la désinformation constitue désormais un risque multidimensionnel**. Ses conséquences ne se limitent ni à la sphère médiatique ni à la réputation des organisations, mais affectent directement leur performance financière, leur fonctionnement opérationnel, leur environnement réglementaire et, à terme, leur capacité à maintenir un avantage compétitif durable.

# Facteurs de vulnérabilité des entreprises face à la désinformation

Les entreprises ne sont pas exposées de manière homogène aux menaces informationnelles. Leur niveau de vulnérabilité dépend d'un ensemble de facteurs structurels, sectoriels et organisationnels qui influencent à la fois leur attractivité en tant que cible et leur capacité de résilience.

### Exposition numérique et médiatique

Les entreprises disposant d'une forte visibilité publique, d'une marque reconnue ou d'une présence importante sur les réseaux sociaux sont davantage susceptibles d'être ciblées. Plus une organisation occupe une place centrale dans l'espace informationnel, plus une campagne hostile bénéficie d'un effet d'amplification.

### Dépendance à la réputation

Certains secteurs, notamment la pharmacie, l'agroalimentaire, la finance, l'énergie ou les technologies, reposent fortement sur la confiance des consommateurs, des investisseurs et des régulateurs. Une atteinte à la réputation peut dès lors produire des effets économiques durables et disproportionnés.

### Cotation boursière

Les entreprises cotées sont particulièrement vulnérables aux opérations de manipulation informationnelle en raison de la sensibilité des marchés financiers aux annonces et aux rumeurs. La diffusion de fausses informations peut entraîner des variations significatives de cours et générer des pertes importantes.

### Sensibilité géopolitique

Les organisations opérant dans des secteurs stratégiques ou dans des environnements géopolitiques tendus sont davantage exposées aux campagnes d'influence conduites par des acteurs étatiques ou para-étatiques. Elles peuvent devenir des cibles indirectes des rivalités économiques et stratégiques internationales.

**Asymétrie informationnelle**

Les entreprises dont les activités sont complexes ou mal comprises du grand public sont plus vulnérables aux narratifs trompeurs. Une faible compréhension de leurs activités favorise la crédibilité des rumeurs et des campagnes de désinformation.

**Préparation organisationnelle insuffisante**

L'absence de dispositifs de veille, de protocoles de gestion de crise ou de formation des collaborateurs constitue un facteur aggravant majeur. Dans ce domaine, la rapidité de détection et de réaction est souvent déterminante pour limiter l'impact d'une attaque.

**Vulnérabilités numériques**

Des dispositifs de communication insuffisamment sécurisés – tels que l'absence de mécanismes d'authentification des courriels, la mauvaise protection des noms de domaine ou des systèmes de communication vulnérables – facilitent les opérations d'usurpation d'identité et de diffusion de faux contenus.

La vulnérabilité d'une entreprise à la désinformation résulte rarement d'un facteur unique. Elle procède généralement de la **combinaison d'une forte exposition informationnelle, d'enjeux réputationnels élevés et d'un niveau de préparation insuffisant face à des menaces de plus en plus sophistiquées**.

Face à la montée des menaces informationnelles, les entreprises les plus résilientes adoptent une **approche intégrée combinant gouvernance, détection, gestion de crise et recours juridiques**. À l'instar du risque cyber, la désinformation doit être appréhendée comme un risque d'entreprise nécessitant des **dispositifs dédiés** et une **coordination transverse**.

- **Une gouvernance intégrée du risque informationnel**

La gestion du risque informationnel ne peut relever d'une seule fonction. Les bonnes pratiques reposent sur une gouvernance associant la direction générale, la communication, le juridique, la sécurité des systèmes d'information et la conformité.

Le comité exécutif assure le pilotage stratégique du risque, tandis que les directions opérationnelles coordonnent respectivement la réponse publique, les actions judiciaires, la détection technique et les obligations réglementaires. Cette approche permet d'intégrer la désinformation dans les dispositifs globaux de gestion des risques.

- **Veille et capacités de détection**

La détection précoce constitue le principal facteur de résilience. Les entreprises renforcent leurs capacités de surveillance à travers des outils de veille médiatique et de social listening, permettant d'identifier rapidement des anomalies de diffusion, des campagnes coordonnées ou des variations inhabituelles de sentiment.

Cette surveillance est généralement complétée par le suivi de l'identité numérique de l'entreprise (noms de domaine, faux comptes, usurpations), l'analyse des forums spécialisés et du dark web ainsi que, de manière croissante, par des solutions de détection de contenus synthétiques et de deepfakes.

- **Protocoles d'alerte et gestion de crise**

La rapidité de réaction est déterminante. Une information fausse non contestée dans les premières heures tend à gagner en crédibilité à mesure de sa diffusion.

Les organisations les plus avancées disposent ainsi de seuils d'alerte prédéfinis, de cellules de crise préconstituées et de scénarios de réponse adaptés aux principales menaces identifiées : faux communiqués, deepfakes de dirigeants, rumeurs sur les produits ou manipulations boursières.

Des exercices réguliers de simulation permettent également de tester les procédures et de renforcer la coordination entre les différentes fonctions concernées.

- **Communication de preuve et authentification de l'information**

Face à une campagne de désinformation, le simple démenti est souvent insuffisant. L'enjeu consiste à produire rapidement des éléments de preuve crédibles permettant de rétablir les faits.

Cette capacité repose notamment sur l'utilisation de dispositifs d'authentification des communications officielles, sur l'existence de relations établies avec les médias, les plateformes numériques et les organismes de vérification de l'information, ainsi que sur la conservation systématique des preuves numériques nécessaires à d'éventuelles procédures contentieuses.

- **Recours juridiques et coopération institutionnelle**

Le volet juridique constitue un complément essentiel de la réponse. Selon la nature de l'attaque, les entreprises peuvent saisir les autorités de régulation compétentes, engager des procédures pour diffamation, usurpation d'identité ou manipulation de marché, ou solliciter le retrait rapide de contenus frauduleux.

À l'échelle européenne, le Digital Services Act (DSA) renforce les obligations des grandes plateformes en matière de traitement des contenus illicites. Les entreprises peuvent également coopérer avec les autorités nationales, les régulateurs sectoriels ou les services spécialisés lorsqu'une campagne présente une dimension criminelle ou transnationale.

Institut
EGA

ISSN : 2739-3283


Institut d'études de géopolitique appliquée
66 avenue des Champs-Élysées, 75008 Paris
Courriel : secretariat@institut-ega.org
Site internet : www.institut-ega.org