RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

VIGINUM

Guide de sensibilisation à **la menace informationnelle** à destination des acteurs économiques français

CDSE
CERCLE DES DIRECTIONS DE LA **SÉCURITÉ** DES **ENTREPRISES**

Secrétariat général de la défense et de la sécurité nationale

Service de vigilance et de protection
contre les ingérences numériques étrangères

Cercle des directions de la sécurité en entreprise, CDSE

Conception / mise en page
Réflexion Graphique
Décembre 2025

Crédit photos
©katemangostar - Freepik
©Luca Bravo, ©Chris Slupski, ©Marten Bjork,
©Pete Stumpf, ©Sumup - Unsplash

Sommaire

Éditorial

Édito de Marc-Antoine BRILLANT, chef du service VIGINUM

Depuis 2021 et la création du service VIGINUM, les menaces de déstabilisation en ligne n'ont cessé de croître à la faveur d'un contexte international dégradé. Ukraine, Roumanie, Moldavie, États baltes, Allemagne, Australie, Canada, pays africains ou de l'Asie du Sud-Est et évidemment la France. Nombreux sont les pays victimes de tentatives de manipulation de l'information. Et si l'on pense assez naturellement aux enjeux électoraux ou de politique étrangère, il s'agit désormais de prendre en compte l'ensemble du spectre visé par la menace informationnelle, notamment nos entreprises, véritable incarnation de la France à l'étranger.

C'est pourquoi je profite de ce guide pour m'adresser à vous, chefs d'entreprise, entrepreneurs et investisseurs : ne croyez pas que cette menace de manipulation ne soit qu'un sujet pour les États ou lors d'élections. Certes la menace représentée par une concurrence toujours plus désinhibée demeure et se durcira probablement. Mais, en tant qu'entreprises françaises, vous êtes susceptibles de faire l'objet de manœuvres de déstabilisation parce qu'au travers de vous, c'est la France et son modèle qui sont visés. Derrière votre réputation, c'est l'image de la France. Derrière votre chiffre d'affaires, ce sont les intérêts économiques français. Malheureusement, pas une semaine ne se passe sans que les équipes de VIGINUM ne détectent une tentative d'ingérence numérique étrangère ou de déstabilisation en ligne visant nos entreprises.

Convaincus de l'impératif de se renforcer ensemble, nous nous sommes associés au Club des directeurs de sécurité des entreprises (CDSE) pour vous apporter une première réponse : ce guide de sensibilisation. Un grand merci aux équipes de VIGINUM et du CDSE, ainsi qu'à son président Cédric Lewandowski, pour leur appui et leur détermination à construire un véritable rempart face aux menaces.

Édito de Cédrick Lewandowski, président du CDSE

La renommée, la confiance et l'image de marque sont au cœur des réussites économiques et commerciales de nos entreprises. La réputation est un bien immatériel qui, si elle est difficile à mesurer et à appréhender, engage cependant l'image que l'entreprise porte dans la société et, par ricochet, sa capacité de dialogue avec les consommateurs.

Les manœuvres des concurrents pour attaquer cet actif immatériel ne sont pas nouvelles, mais l'avènement de la société numérique et l'interrelation croissante entre le domaine politique et économique renforcent les menaces pour nos entreprises. La digitalisation crée ainsi un paradigme qui nous conduit vers un monde où la post-vérité pourrait malheureusement devenir la norme.

Dans ce contexte, attaquer la réputation d'une entreprise est devenu un moyen relativement facile de saboter sa réussite économique, tout en limitant le risque de poursuites judiciaires. Ce mouvement est facilité par l'anonymat permis par internet, et notamment sur les réseaux sociaux, qui permet à des concurrents, des acteurs criminels, voire des États, d'agir sans forcément être identifiés et donc poursuivis.

Dans une période marquée par l'hybridation des menaces, comme le détaille la nouvelle Revue nationale stratégique de 2025, les entreprises peuvent être la cible des enjeux de puissance, avec des États cherchant, par l'intermédiaire de modes opératoires hybrides, à atteindre d'autres États via la déstabilisation de leur secteur économique. Il s'agit donc de renforcer la vigilance collective et de développer, sur ce sujet, un partenariat public-privé efficace, permettant de renforcer le continuum de sécurité.

C'est pourquoi nous sommes ravis de co-produire ce guide avec VIGINUM, signe du renforcement constant des liens entre le CDSE et l'État, au service de la sécurité nationale et de la sécurité de nos entreprises.

Présentation du guide

À quoi sert ce guide ?

Ce guide de sensibilisation a pour but de dresser un panorama de la menace informationnelle, notamment appliquée au champ économique, afin de faire prendre conscience de la menace et de ses enjeux. Ce guide a également pour vocation de partager des réflexes et des bonnes pratiques pour aider les entreprises à mieux détecter et, le cas échéant, réagir aux manipulations de l'information qui les ciblent.

À qui s'adresse-t-il ?

De par son caractère transverse et sa manifestation en ligne sur les réseaux sociaux et les sites web, la menace informationnelle et les recommandations associées concernent tous les échelons et toutes les fonctions d'une entreprise.

Quel est le rôle de VIGINUM dans la protection des intérêts économiques français ?

Créé le 13 juillet 2021 et rattaché au Secrétariat Général de la Défense et de la Sécurité Nationale, VIGINUM est le service de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères. Ce service à compétence nationale a pour mission principale de détecter et de caractériser les opérations et campagnes de manipulation de l'information sur les plateformes numériques, impliquant des acteurs étrangers dans le but de nuire à la France et à ses intérêts.

Pour ce faire, le service étudie les phénomènes inauthentiques sous un angle technique afin d'y discerner notamment les comportements anormaux ou coordonnés exploitant les services des plateformes numériques.

Les actifs économiques, scientifiques et industriels majeurs français relèvent des intérêts fondamentaux de la Nation. À ce titre, VIGINUM est compétent pour détecter et caractériser les campagnes numériques de manipulation de l'information impliquant des acteurs étrangers et visant des entreprises françaises.

La menace informationnelle à l'encontre des entreprises françaises

Un contexte géopolitique volatil ciblant les entreprises françaises

Le contexte géopolitique actuel, défini par l'exacerbation des tensions internationales et la persistance de conflits armés déstabilisateurs, favorise une mise en concurrence accrue entre compétiteurs internationaux qu'ils soient étatiques ou non-étatiques. Ces rivalités se traduisent notamment par la mise en œuvre de manœuvres informationnelles ciblant le tissu économique des États. Ainsi, dans ce contexte, les entreprises françaises ne sont pas uniquement appréhendées comme de simples entités commerciales mais représentent directement ou indirectement les intérêts stratégiques de la France. Cette incarnation peut s'expliquer notamment en raison de :

- **l'origine considérée comme française :** une entreprise dont le siège social est basé en France ou dont le capital est majoritairement détenu par des acteurs français est susceptible d'être associée aux intérêts économiques français ;
- **le positionnement sectoriel :** les entreprises stratégiques ou critiques peuvent être symboliquement représentatives des capacités industrielles ou technologiques de la France ;
- **les liens avec les pouvoirs publics :** certaines entreprises, du fait de leurs contrats avec l'État, de partenariats institutionnels ou d'une participation directe de l'État à leur capital peuvent renforcer l'incarnation des intérêts français ;
- **les dirigeants :** certains profils de dirigeants d'entreprises - personnalités emblématiques du monde économique français, anciens hauts fonctionnaires, militaires ou personnalités issues des grands corps de l'État - peuvent suggérer une proximité avec les sphères gouvernementales françaises.

Ainsi, certains compétiteurs ou puissances concurrentes, en ciblant les entreprises françaises dans le champ informationnel, cherchent par rebond à viser les intérêts français. Cette porosité entre intérêts économiques privés et intérêts stratégiques étatiques fait des entreprises françaises des cibles de choix de la lutte informationnelle adverse, devenue une expression de rapports de force entre puissances.
Les entreprises françaises peuvent ainsi être ciblées par une diversité d'acteurs : groupes militants, clients mécontents, concurrents mais également des puissances étatiques à la conquête de certains marchés ou en défense de leurs intérêts. Ces différents acteurs peuvent agir de façon planifiée, coordonnée ou par simple opportunisme.

Qu'est-ce que la menace informationnelle en ligne et la notion d'ingérence numérique étrangère ?

Composante à part entière des menaces dites « hybrides », la menace informationnelle en ligne se définit par l'expression d'une intentionnalité malveillante dans le champ informationnel à travers la conduite de manœuvres ou de campagnes numériques de manipulation de l'information. Elle peut donc relever de la propagande, de l'influence, ou encore de la communication stratégique, jusqu'à constituer une ingérence numérique étrangère.
Placée au cœur de la mission de VIGINUM, l'ingérence numérique étrangère répond à quatre critères :

> **son contenu :** allégations ou imputations de faits manifestement inexactes ou trompeuses ;

> **son comportement :** l'usage de moyens inauthentiques ou coordonnés (bots[1], trolls, faux comptes, sponsorisation de contenus, etc.) ;

1. L'ensemble des termes techniques utilisés sont définis en annexe de ce guide.

> **sa finalité :** l'atteinte aux intérêts fondamentaux de la Nation ;

> **ses auteurs :** l'implication directe ou indirecte d'un acteur étranger (étatique, paraétatique ou non étatique).

L'INGÉRENCE NUMÉRIQUE ÉTRANGÈRE SE DISTINGUE DONC DE LA DÉSINFORMATION ET DES « FAKE NEWS » DONT LE POINT COMMUN EST DE PROPAGER DE FAUSSES INFORMATIONS VERS LE GRAND PUBLIC.

Ainsi, **les campagnes numériques de manipulation de l'information et l'ingérence numérique étrangère doivent être différenciées de la crise communicationnelle ou d'*e-réputation***, car elles présentent plusieurs caractéristiques d'inauthenticité et de manipulation :

> elles se déploient généralement de manière dissimulée et non revendiquée, ce qui rend son auteur difficilement identifiable ;

> elles impliquent un mode opératoire coordonné et structuré contribuant à l'amplifier artificiellement en ligne ;

> elles ont pour finalité principale la déstabilisation de l'entité ciblée afin de servir les intérêts du commanditaire de la manœuvre.

Devenues de véritables instruments de déstabilisation des démocraties, les ingérences numériques étrangères reposent sur des stratégies et des techniques visant à modifier les comportements collectifs avec pour objectif principal d'éroder la confiance du public dans les institutions, de polariser les débats d'intérêt général ou de créer voire d'amplifier des tensions au sein des populations.
Aujourd'hui la menace informationnelle s'immisce dans tous les champs du débat public numérique, exploitant des faits d'actualités ou de société marquants dans le but d'altérer la sincérité des échanges.

Quelles évolutions de la menace informationnelle en ligne ?

La menace informationnelle en ligne s'est largement complexifiée et diversifiée ces dernières années :

- désormais, les acteurs de la menace s'appuient sur des modes opératoires informationnels plus **sophistiqués** incluant le recours à l'intelligence artificielle générative d'images ou de textes et permettant de s'adapter à des contextes linguistiques et culturels précis ;
- elle est également davantage **dissimulée** et marquée par la recherche de proxies et d'intermédiaires à des fins de « désilhouettage ». Cette sous-traitance accrue au profit de réseaux informels ou d'acteurs privés du marketing digital et de la communication contribue de facto à dissimuler les véritables commanditaires ;
- enfin, les acteurs étrangers à l'œuvre n'hésitent plus à coupler des opérations **planifiées sur le long terme** avec des manœuvres opportunistes afin d'exploiter tout sujet de société ou d'actualité.

Cette complexification produit également des **effets sur le champ économique** avec des manœuvres informationnelles soigneusement conçues et plus difficiles à détecter à l'encontre des entreprises, d'où la nécessité de se renforcer pour s'en prémunir.

Comment se matérialise-t-elle ?

S'agissant du champ économique, la menace informationnelle peut prendre la forme d'opérations planifiées ou d'actions opportunistes, conduites par des acteurs étatiques ou non-étatiques. Ces acteurs peuvent concevoir et diffuser des contenus hostiles à l'entreprise ou contribuer à en amplifier des existants afin de leur conférer davantage de visibilité.

Les entreprises et l'activité économique françaises sont ainsi régulièrement la cible de campagnes de dénigrement et d'appels au boycott sur les réseaux sociaux, espaces propices aux polémiques sociétales, à la « viralisation » des contenus et aux mobilisations.

Depuis sa création, VIGINUM observe que les manœuvres informationnelles menées par des acteurs étrangers et ciblant les entreprises sont en augmentation. La majorité des acteurs étrangers de la menace ont en effet largement investi le champ économique afin d'y diffuser des logiques narratives en lien avec la défense ou la promotion de leurs intérêts stratégiques.

Les investigations de VIGINUM révèlent par ailleurs une grande diversité des secteurs d'activité ciblés. Les entreprises ayant fait l'objet de manœuvres informationnelles ne se cantonnent pas aux domaines dits « régaliens » (défense, énergie, aérospatial) mais appartiennent également au secteur des industries de consommation (grande distribution, textile, agro-alimentaire, télécommunications, etc.).

Enfin, les acteurs de la menace investissent une grande diversité de plateformes en ligne, sélectionnées selon les audiences ciblées, et ont recours aux infrastructures Internet pour conduire leurs manœuvres informationnelles.

L'aggravation des tensions internationales, la forte exposition des intérêts économiques français dans certaines zones de crise et les nouveaux usages numériques en matière d'information rendent la menace informationnelle à la fois persistante et facile d'emploi. Ces observations font craindre une hausse de la menace informationnelle ciblant le secteur économique et appellent à un regain de vigilance.

Exemples de techniques ayant ciblé des entreprises françaises

En matière de menace informationnelle, VIGINUM observe que les entreprises et les acteurs économiques sont ciblés par les principales techniques suivantes :

> Raid numérique ou « astroturfing »

Cette technique consiste à créer ou amplifier un *bad buzz* autour d'un sujet polémique lié à l'entreprise, généralement *via* l'utilisation d'un mot clé ou de plusieurs *hashtags*, dont les acteurs malveillants vont chercher à augmenter la visibilité.
Dans le champ économique, des contenus hostiles à l'entreprise peuvent être générés puis amplifiés de manière coordonnée et inauthentique par des publications multi-plateformes, des *trolls* et/ou des réseaux de *bots* appuyés par des médias affiliés à un acteur étranger.

Dans le contexte de la guerre d'agression russe en Ukraine, VIGINUM a ainsi observé qu'un groupe de la grande distribution française a été la cible d'un raid numérique sur X pour avoir maintenu son implantation géographique et son activité commerciale en Russie. Des mouvances d'activistes pro-ukrainiennes en ligne se sont mobilisées afin de diffuser massivement des hashtags appelant au boycott des produits de l'entreprise, accusée de participer à un effort de guerre.

> L'incitation à conduire des actions dans le champ physique

Cette technique consiste à appeler en ligne à conduire des actions dans l'espace public, comme inciter à l'organisation de manifestations ou des dégradations (saccage, vandalisme, etc.) mais aussi influer sur la consommation.
Dans le champ économique, elle est utilisée pour appeler à manifester devant des locaux d'entreprises, voire à les dégrader. Elle se traduit également par des appels au *boycott* en ligne qui sont suivis d'actions visant à nuire aux produits des marques concernées et à empêcher leur consommation. Les effets produits dans le champ physique peuvent ensuite être instrumentalisés et amplifiés dans le champ informationnel à des fins de propagande, alimentant une boucle informationnelle.

Dans le contexte de la guerre d'agression russe en Ukraine, VIGINUM a détecté la diffusion de contenus par une association pro-russe appelant à des rassemblements devant plusieurs implantations d'un groupe industriel français sur le territoire national. Ces publications, accompagnées de supports visuels et de hashtags, ont été rediffusées par des relais d'influence pro-russes, laissant ainsi présumer d'une action coordonnée. Dans un second temps, l'appareil de propagande d'État russe a instrumentalisé en ligne ces manifestations afin d'en amplifier la portée, dans la perspective de saper le soutien politique apporté par la France à l'Ukraine.

> Recours à des médias et/ou des influenceurs

Cette technique consiste à amplifier la diffusion d'un contenu en ligne en utilisant des médias ou des comptes disposant d'une forte audience qui s'adressent à leur communauté de manière régulière sur des thématiques précises. L'influenceur ou le média est ainsi identifié comme un expert de son sujet de prédilection, ou comme une source d'information fiable ou d'inspiration.

Dans le champ économique, les comptes d'influenceurs ou les médias sont susceptibles d'être approchés par des acteurs étrangers malveillants à la recherche de vecteurs de diffusion de manipulation d'information ou de propagande ciblant l'entreprise.

Dans le contexte des tensions entre la France et le Niger, VIGINUM a détecté une manœuvre informationnelle articulée en plusieurs étapes ayant ciblé une entreprise du secteur de l'énergie française. Dans un premier temps, de fausses informations relatives à l'entreprise ont été diffusées sur une chaîne YouTube inconnue. Ce narratif a ensuite été repris par des médias africains affiliés à des dispositifs d'influence numérique étrangers et qui publient des articles contre rémunération. Ces articles, qui contribuent à donner une légitimité à l'information, ont à leur tour été repris sur les plateformes par des chaînes affiliées à des dispositifs numériques étrangers.

> Décontextualisation et détournement de visuels

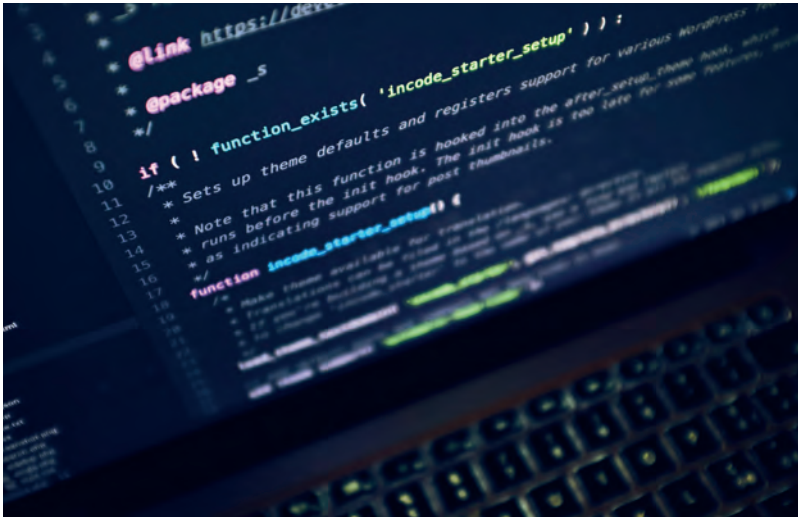
Cette technique consiste à extraire un visuel (image, vidéo, etc.) de son contexte originel, voire le détourner, pour l'utiliser dans le but de tromper les audiences. Ce procédé vise à exagérer ou fausser l'événement en cours afin de susciter davantage d'émotions auprès de l'audience visée.
Dans le champ économique, cette technique peut être utilisée par un acteur malveillant pour attribuer à une entreprise de fausses actions ou déclarations.

VIGINUM a détecté la primo-diffusion sur la plateforme Telegram d'une vidéo contrefaite d'un média national français suggérant une corrélation entre la vente d'une filiale d'un groupe pharmaceutique national et les intérêts personnels d'une figure politique étrangère. Si cette vidéo reprend le début d'une émission authentique de la version anglophone du média français, la suite est détournée et diffuse des narratifs trompeurs relatifs à l'opération de rachat ainsi qu'à l'activité commerciale du protagoniste. Cette vidéo a ensuite été reprise sur les plateformes par des chaînes affiliées à des dispositifs numériques étrangers.

> Usurpation d'identité et *typosquatting*

Cette technique consiste à usurper l'identité d'une entreprise, de ses porte-paroles ou de ses dirigeants pour véhiculer de fausses informations pouvant leur nuire. Ce procédé peut s'appuyer sur le *typosquatting* qui consiste à enregistrer un nom de domaine délibérément mal orthographié du site web de l'entreprise afin de tromper les internautes et diffuser des narratifs trompeurs. Cela peut nuire à la réputation de l'entreprise, tromper ses clients ou partenaires et causer des perturbations économiques.

La diffusion de fausses informations portant sur les enjeux financiers sensibles via plusieurs faux communiqués de presse publiés sur le site miroir (usurpé) d'une entreprise, ensuite repris par une agence de presse financière, ont entraîné une forte chute du titre en Bourse. Si les auteurs de cette manipulation boursière n'ont pas été identifiés, cette technique pourrait être reproduite à des fins de déstabilisation par un acteur étranger.



Quels sont les impacts potentiels ?

La menace informationnelle peut avoir, sur l'entreprise, plusieurs types d'impacts :

> Impact réputationnel

L'acteur malveillant peut chercher à atteindre la réputation de l'entreprise en délégitimant ou décrédibilisant ses actions, ses produits ou les déclarations publiques de ses dirigeants sur la base d'informations critiquant le plus souvent son intégrité ou ses responsabilités sociale, sociétale ou environnementale.
De nature principalement opportuniste, ces actions peuvent remettre en cause l'intégrité de l'entreprise et provoquer une baisse de son chiffre d'affaires. Les conséquences sur le plan réputationnel sont considérées comme souvent immédiates et susceptibles de s'inscrire dans la durée, la restauration de l'image de l'entreprise et le relèvement financier pouvant prendre du temps.

> Impact économique

L'acteur malveillant peut chercher à provoquer des retombées économiques de sa campagne numérique de manipulation de l'information en appelant au boycott de ses produits.
Cette action peut avoir des conséquences majeures sur le développement économique de l'entreprise avec des pertes de marchés, de clients, de partenaires ou de prospects commerciaux, mais aussi une chute de l'action en bourse conduisant à des pertes financières, des défauts de trésorerie voire des difficultés de remboursement ou d'acquisitions de biens.
Les manœuvres informationnelles visant à produire un impact économique peuvent également altérer la perception qu'ont les partenaires commerciaux, les investisseurs ou les prospects de l'entreprise et générer une perte de confiance susceptible de freiner les opportunités de collaboration, d'investissement ou de croissance. Ce discrédit perçu, même temporaire, peut ralentir ou bloquer des négociations en cours, retarder l'accès à de nouveaux marchés ou détourner des partenaires vers des

concurrents perçus comme davantage fiables ou éthiques. La suspicion et le climat de défiance consécutifs à la campagne numérique de manipulation de l'information peuvent s'inscrire dans la durée et sont parfois difficiles à inverser.
L'impact économique peut ainsi découler de l'impact réputationnel.

> Impact sécuritaire

La campagne de manipulation de l'information peut provoquer ou amplifier un trouble à l'ordre public en lien avec l'entreprise ciblée. L'acteur malveillant peut chercher à organiser des manifestations dans la « sphère physique » en appelant à des rassemblements devant des locaux d'entreprise ou en incitant à leur dégradation, augmentant dès lors le risque d'affrontements, de violences ou de dégâts matériels. Il peut s'agir d'incitations à bloquer l'accès aux locaux, à vandaliser les bâtiments, ou à perturber les activités économiques de l'entreprise avec des conséquences potentielles sur son fonctionnement.
Ces manœuvres peuvent alors créer un climat d'insécurité, de tension ou de peur et sont susceptibles d'affecter la sécurité physique des locaux de l'entreprise mais également de ses employés ou des clients.
Ces actions menées dans des lieux publics peuvent dans un second temps faire l'objet d'une couverture amplifiée dans le champ informationnel par des relais d'influence et appareils de propagande d'État qui vont récupérer ces actions en cherchant à leur conférer une visibilité disproportionnée.
L'impact sécuritaire ne se limite donc pas aux perturbations immédiates sur le terrain mais peut engendrer une dégradation durable de la confiance du public, une fragilisation des capacités de gestion des risques de l'entreprise et à une possible déstabilisation plus générale de l'ordre public.

> Impact de « déstabilisation interne »

La campagne numérique de manipulation de l'information peut altérer la perception qu'a l'écosystème - employés, partenaires, investisseurs - de l'identité, des valeurs ou des engagements de son entreprise.
Une attaque informationnelle remettant en question l'adhésion de l'entreprise aux valeurs qu'elle affiche peut notamment saper la confiance de son écosystème. Le socle de valeurs partagées peut se retrouver fragilisé et favoriser l'émergence d'une crise de gouvernance interne : les collaborateurs peuvent se sentir trahis ou instrumentalisés, les partenaires sont susceptibles de se désolidariser, les clients peuvent vouloir se détourner de la marque, etc.
L'attaque informationnelle est également susceptible d'altérer le fonctionnement interne de l'entreprise en mobilisant des ressources pour y faire face, générant ainsi une charge de travail supplémentaire et du stress pour les équipes.
En s'attaquant aux valeurs d'une entreprise, une attaque informationnelle peut alors altérer la cohésion interne, ébranler l'adhésion des parties prenantes, ralentir le niveau de décision et, de surcroît, compromettre la stabilité du modèle économique.

> *Dans ce nouveau paradigme, l'entreprise devient une cible pour des acteurs étatiques non seulement pour ce qu'elle fait mais aussi pour ce qu'elle est, son origine, ses valeurs, sa culture et ce qu'elle représente. L'entreprise doit ainsi s'adapter à ces nouvelles contraintes, en comprendre les mécanismes, bâtir ses propres solutions pour conserver son agilité, sa sérénité et son indépendance en transformant ces risques en opportunités.*

Pierre Tramier,
président de la commission
« *Radicalisations* » du CDSE

Les préconisations de VIGINUM

Anticiper la menace pour s'en protéger

> Sensibiliser à la menace

La sensibilisation est la clé de voûte de la prévention. Sensibiliser vise à informer et à faire prendre conscience de la réalité de la menace informationnelle, et du risque qu'elle peut faire peser sur une entreprise et ses collaborateurs. Cette sensibilisation doit concerner autant les membres du COMEX que les échelons intermédiaires et opérationnels, qui sont tous susceptibles de détecter une menace informationnelle ou d'en être la cible.
L'organisation de sessions de sensibilisation pour vos collaborateurs et/ou la mise en place d'un espace d'information interne en ligne pourra faciliter cette appréhension de la menace.

> Adapter votre organisation à la menace

Face à la menace informationnelle qui peut toucher votre entreprise, il est nécessaire d'anticiper et de prendre en compte cette menace dans vos processus existants, pour s'en prémunir.
Par ailleurs, un dispositif d'alerte peut être mis en place pour faciliter les signalements internes.

1. À l'intérieur de votre entreprise

> **Mettre en place une veille** sur les échéances, événements, problématiques et actions sensibles liées à votre organisation et votre secteur d'activité, susceptibles d'être instrumentalisés en ligne afin de porter atteinte à votre réputation.

> **Définir un dispositif interne de réponse,** réactif et coordonné entre toutes les fonctions. Il est notamment important :

- **d'identifier un point de contact/référent qui serait propriétaire du sujet.** Ce point de contact sera en charge de la sensibilisation, de définir les processus les plus adaptés et de coordonner la réponse collective, en s'assurant d'une bonne répartition des rôles et de la fluidité du dialogue entre toutes les fonctions, dont les équipes en charge de la veille ;
- **d'adapter vos processus existants** de façon à prendre en compte la menace informationnelle.

> **Intégrer des aspects informationnels aux scénarios des exercices de crise organisés dans votre entreprise**, afin d'éprouver le fonctionnement de l'ensemble du dispositif face à la menace informationnelle et de vérifier que les acteurs en interne sont bien identifiés.

> **Capitaliser sur les retours d'expérience (vécue ou simulée en exercice)** pour identifier les points de blocage à lever.

2. À l'extérieur de votre entreprise

> **Identifier les communautés, parties prenantes et relais d'influence utiles**, auprès desquels communiquer (clients, prestataires, autorités, médias, etc.).

> **Créer un fichier de contacts** actualisé et recourir à une méthode de diffusion éprouvée (par exemple avec l'utilisation systématique d'une unique liste de diffusion par mail ou d'une boucle de messagerie instantanée dédiée avec les contacts pertinents afin de pouvoir diffuser très rapidement des informations officielles) ;

> **Contacter VIGINUM en cas de besoin.** Le service accompagne les entreprises françaises ciblées par les attaques informationnelles qui relèveraient de l'ingérence numérique étrangère. Le service invite les entreprises à signaler les contenus malveillants par le canal de communication établi au préalable ou à l'adresse dédiée : viginum_signalement@sgdsn.gouv.fr

Faire face à la menace informationnelle

> S'interroger sur la nature et la portée de l'incident

Bien réagir, c'est d'abord se poser la question de « quand » réagir et sur quels sujets.
L'espace informationnel numérique, en particulier les réseaux sociaux, est saturé par un grand nombre d'informations pouvant être manipulées. Néanmoins, **la diffusion d'une information manipulée n'engendre pas nécessairement de crise.** Il convient donc de :

> **prioriser les sujets à traiter**, à la fois pour ne pas s'épuiser en tentant de répondre à tout ce qui serait observé lors de la veille des plateformes en ligne, mais aussi pour **éviter de donner de la visibilité à des contenus qui n'en auraient pas forcément eu autrement ;**

> **être vigilant vis-à-vis des métriques affichées par les plateformes**, c'est-à-dire des indicateurs liés à la viralité et à l'engagement autour d'un contenu (nombre de vues, engagement, likes, partages, etc.).

Les métriques affichées par les plateformes peuvent certes donner une idée générale de la visibilité d'un contenu, mais ces derniers n'en restent pas moins des indicateurs imparfaits notamment car :

> ces indicateurs sont manipulables, et souvent manipulés dans le cadre des manœuvres informationnelles étudiées par VIGINUM (nombre de vues YouTube artificiellement augmentées, faux commentaires, etc.)

> ces indicateurs sont différents d'une plateforme à l'autre, de même que les usages : une vue sur TikTok n'est par exemple pas calculée de la même façon qu'une vue sur Youtube. Ou encore un *like* est moins engageant sur TikTok qu'un *like* sur Twitter/X.

> **se questionner**, au-delà de la visibilité et de la viralité telles que définies par les indicateurs clés de performance pour déterminer s'il est opportun de réagir à un contenu diffusé en ligne.

Exemples de questions à se poser :

✓ Le phénomène porte-t-il sur un sujet de vulnérabilité pour l'organisation ?

✓ Le phénomène vise-t-il à amplifier des narratifs préexistants ayant déjà donné lieu à des crises ?

✓ Le phénomène présente-t-il des appels à l'action ?

✓ Sur combien de plateformes le phénomène observé est présent, en combien de langues ?
Est-il présent sur des plateformes particulièrement utilisées par la population ?

✓ Est-il repris par des relais influents ?

S'interroger sur ces différents paramètres permettra de réaliser un état des lieux plus fin de la situation et de déterminer s'il y a lieu d'apporter une réponse au niveau de l'entreprise, en s'appuyant sur les relais pertinents, préalablement identifiés.

> Connaître les moyens juridiques à votre disposition

La liberté d'information et de communication est un principe très établi dans l'ordre juridique français.

En matière pénale, seuls certains cas de fausses nouvelles peuvent être réprimés. Dans les cas prévus par la loi, la seule fausseté de la nouvelle ne suffit pas : il convient de caractériser une atteinte à un intérêt (public ou personnel) et un lien de causalité entre la fausseté de la nouvelle et l'atteinte à cet intérêt.

Parmi les infractions prévues, il convient de noter les suivantes, dont certaines peuvent être mobilisées. Elles n'ont cependant pas vocation, compte tenu du temps judiciaire, à être des outils de remédiation pendant la partie la plus aiguë de la crise informationnelle.

- **Délit de « fausse alerte »** (typiquement, fausse alerte à la bombe ou au sinistre) : **article 322-14 du code pénal.**
- **Délit de publication de montages d'images ou de paroles** sans indiquer qu'il s'agit de montage : **article 226-8 du code pénal** (ce délit peut notamment comprendre les fausses vidéos d'une personne générée par IA qui ne l'indiquent pas spécifiquement).
- **Délit de fausse nouvelle** ayant troublé la paix publique : **article 27 de la loi de 1881** sur la liberté de la presse (mais il faut démontrer un lien de causalité ou un risque direct). Cette infraction n'est presque jamais utilisée, et rarement avec succès. Elle a cependant pu être mobilisée contre des campagnes anti-vaccination trompeuses, pendant l'épidémie de Covid.

Outre le champ de l'action pénale, les voies civiles, et notamment le code de la propriété intellectuelle, peuvent également s'avérer pertinentes.

En cas de crise informationnelle, votre direction juridique devra être saisie afin d'envisager de recourir à ces moyens juridiques.

Glossaire

> ***ASTROTURFING*** : mode opératoire consistant à conférer de la visibilité à un sujet en faisant croire qu'il est un phénomène de masse alors même qu'il émane de la coordination de quelques comptes produisant un volume important de publications sur un même sujet.

> ***BOT*** : programme informatique automatisé pour simuler le comportement humain sur les réseaux sociaux. Un *bot* est capable de faire des publications, de laisser des commentaires, de partager ou d'aimer d'autres publications.

> ***COPY-PASTA*** : bloc de texte ou de visuel copié-collé à l'identique ou presque, sur une ou plusieurs plateformes *web*, dans le but d'amplifier la visibilité d'un message.

> ***DEBUNKING*** : dévoiler ou discréditer des revendications ou informations fausses ou exagérées.

> ***DEEPFAKE*** : trucage audio ou vidéo à partir d'éléments existants, utilisant l'intelligence artificielle pour changer le visage d'une personne dans une vidéo ou reproduire sa voix.

> **DÉSINFORMATION** : diffusion d'informations inexactes dans le but de tromper et de causer un préjudice.

> **ENGAGEMENT** (sur les réseaux sociaux) : pourcentage des personnes qui ont aimé, commenté et partagé une publication sur les réseaux sociaux après l'avoir vue.

> ***FACT-CHECKING*** : processus par lequel une information livrée dans l'espace public est vérifiée dans le but d'en prouver sa véracité ou non.

> ***HASHTAG*** : mot-clé cliquable, précédé du signe dièse (#), permettant de faire du référencement sur les sites de microblogage.

> **INGÉRENCE NUMÉRIQUE ÉTRANGÈRE** : volet numérique de la manipulation de l'information, elle consiste pour un État étranger ou une entité non-étatique étrangère, à diffuser de manière artificielle ou automatisée, massive et délibérée des contenus manifestement inexacts ou trompeurs, susceptibles de porter atteinte aux intérêts fondamentaux de la Nation.

> **MALINFORMATION** : la malinformation est une information qui se fonde sur la réalité, mais qui est sortie de son contexte ou partielle.

- **MANIPULATION DE L'INFORMATION :** ensemble des actions hostiles visant à diffuser intentionnellement et de manière massive des nouvelles falsifiées, inexactes (désinformation) ou encore associées à de vraies informations pour les rendre crédibles, sorties de leur contexte ou partielles (malinformation). Notion surtout utilisée à l'international (ex. : OTAN) pour désigner l'ensemble des actions de désinformation et de malinformation.
- **MENACE INFORMATIONNELLE :** expression d'une intentionnalité malveillante dans le champ informationnel se traduisant par la conduite de manœuvres ou de campagnes numériques de manipulation de l'information.
- **MENACE HYBRIDE :** une menace hybride désigne l'ensemble des effets produits par l'emploi coordonné, ambigu et évolutif de moyens militaires et non militaires, légaux ou illégaux, directs ou indirects, par un acteur étatique ou non étatique, dans le but de perturber, contraindre ou affaiblir la France et ses partenaires, tout en restant en-deçà des seuils traditionnels de conflit armé ou de riposte.
- **MÉSINFORMATION :** la mésinformation est une information qui est fausse, mais que la personne la diffusant pense vraie.
- **MODE OPÉRATOIRE INFORMATIONNEL :** selon VIGINUM, ensemble de comportements, d'outils, de tactiques, techniques et procédures 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.
- **OSINT :** ensemble de pratiques d'investigation visant à dévoiler une information préalablement dissimulée en récoltant, croisant ou analysant des données numériques disponibles en source ouverte.
- ***TROLL* :** comptes ou groupes de comptes qui, par jeu, moquerie ou activisme politique, perturbent l'espace numérique en cherchant à déstabiliser les débats publics.
- ***TYPOSQUATTING* :** technique qui consiste à enregistrer des noms de domaines avecdes URL délibérément mal orthographiés de sites *web* connus pour tromper des internautes peu avertis.

Secrétariat général de la défense et de la sécurité nationale

viginum_signalement@sgdsn.gouv.fr