RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

VIGINUM

Guide de sensibilisation à la **menace informationnelle**

Ecosystème des acteurs économiques associés aux Jeux Olympiques et Paralympiques de Paris 2024

Secrétariat général de la défense et de la sécurité nationale

Service de vigilance et de protection contre
les ingérences numériques étrangères

Conception :
VIGINUM
Mai 2024

Qu'est-ce que la menace informationnelle ?

Composante à part entière des menaces «dites hybrides», la menace informationnelle en ligne impliquant des acteurs étrangers, se traduit par des **manœuvres** ou de **campagnes numériques de manipulation de l'information**, avec pour objectifs de **porter atteinte aux intérêts de l'entité ciblée** et/ou **promouvoir les revendications** d'un acteur.

Prenant la forme d'opérations planifiées ou d'actions opportunistes, ces manœuvres cherchent à **diffuser** de **fausses informations** ou à **amplifier des contenus malveillants déjà présents dans le débat public**.

S'appuyant sur un contexte géopolitique marqué par l'exacerbation des tensions internationales et la recherche du rapport de force, les campagnes numériques de manipulation de l'information sont devenues un **véritable instrument de déstabilisation des démocraties**.

En 2024, la France accueillera du 26 juillet au 8 septembre les Jeux Olympiques et Paralympiques de Paris 2024. Les compétitions seront suivies par près de 4 milliards de téléspectateurs. Leur couverture médiatique offrira une **surface d'exposition informationnelle inédite** aux acteurs étrangers malveillants désireux d'affecter les intérêts économiques entourant les événements.

Comment cette menace se matérialise-t-elle ?

En matière de menace informationnelle, les entreprises et acteurs économiques peuvent être ciblés par les principaux modes opératoires suivants :

Le *raid* numérique

Ce mode opératoire vise à créer ou amplifier un *bad buzz* autour d'un sujet polémique, généralement *via* l'utilisation d'un mot clé ou de plusieurs hashtags, dont les acteurs vont chercher à en augmenter la visibilité. Le recours à la création et au **partage massif d'images**, telles que des **détournements de logos**, permet une meilleure diffusion des narratifs. Les contenus hostiles à l'entreprise peuvent parfois être 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.

L'incitation à conduire des actions dans le champ physique

Ce mode opératoire peut se traduire en ligne par des **appels à manifester ou à dégrader des locaux** d'entreprises ciblées. Les effets produits dans la vie réelle peuvent, par la suite, être instrumentalisés dans le champ informationnel à des fins de **propagande**. Par ailleurs, les appels au boycott en ligne peuvent être suivis d'actions visant à **nuire aux produits des marques** concernées et à empêcher leur consommation.

L'usurpation d'identité

Ce mode opératoire consiste pour l'acteur malveillant à **usurper l'identité d'une entreprise**, de ses porte-paroles ou de ses dirigeants pour véhiculer de **fausses informations** pouvant leur nuire auprès de relais d'opinion influents.

Quels sont les risques encourus ?

La menace informationnelle peut poser, pour les acteurs économiques ciblés, les risques suivants :

- **un risque réputationnel** consécutif à la conduite d'une campagne de manipulation de l'information ou d'une manœuvre informationnelle visant **à atteindre l'image de l'entreprise ciblée** en délégitimant ou décrédibilisant ses actions, ses produits ou les déclarations publiques de ses dirigeants ;

- **un risque économique** consécutif à la conduite d'une campagne de manipulation de l'information ou d'une manœuvre informationnelle visant **à affecter les intérêts économiques de l'entreprise ciblée**, en appelant au boycott de ses produits ou en entraînant une chute de l'action en bourse ;

- **un risque sécuritaire** consécutif à la conduite d'une campagne de manipulation de l'information ou d'une manœuvre informationnelle visant **à amplifier, instrumentaliser ou provoquer un trouble à l'ordre public** en lien avec l'entreprise ciblée.

Comment se protéger ?

Pour l'organisation

Sensibiliser :

- La sensibilisation vise à informer et à faire prendre conscience de la réalité de la menace informationnelle, et ainsi du risque qu'elle peut faire peser sur une organisation. Cette sensibilisation doit concerner autant les échelons de direction que l'ensemble des collaborateurs.

Anticiper :

- Identifier les communautés, parties prenantes et relais d'influence utiles en amont d'une gestion de crise.
- Identifier les sujets, thématiques ou événements susceptibles d'être manipulés.

Se préparer :

- Rapprocher les fonctions communication, sécurité/sûreté et systèmes d'information afin de faciliter les interactions lors d'une crise. Mettre en place un dispositif interne de réponse, réactif et coordonné entre toutes les fonctions de l'entreprise.
- Définir une stratégie de communication de crise, fondée sur des cas concrets d'atteinte réputationnelle.
- Organiser des exercices de gestion de crise, prenant en compte les aspects informationnels.

Pour le collaborateur

- Vérifier la source de l'information qui circule.
- Ne pas relayer une information que vous n'avez pas vérifiée.
- Ne pas répondre à une fausse information qui toucherait votre entreprise.
- Signaler les contenus qui vous semblent faux, trompeurs ou inexacts aux équipes compétentes.

Qu'est-ce que VIGINUM ?

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. Il a pour mission principale de détecter et de caractériser les 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 : comptes suspects, contenus malveillants, comportements anormaux ou coordonnés qui se manifestent sur les plateformes numériques.

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

Si vous pensez que votre entreprise est victime d'une campagne numérique de manipulation de l'information relevant de l'ingérence numérique étrangère,
contactez VIGINUM : **viginum_signalement@sgdsn.gouv.fr**

Secrétariat général de la défense et de la sécurité nationale

viginum_signalement@sgdsn.gouv.fr