Guide pour décrypter la désinformation.

Guide étape par étape pour identifier les principaux campagnes des attaques de désinformation ciblant les journalistes et les médias

Guide Rapide

Voici quatre étapes clés que les journalistes, les chercheurs et toute autre personne effectuant un travail d'enquête sur les campagnes de désinformation menées contre les médias doivent suivre :

1. **Comprendre le contexte**
2. **Analyser la chronologie, le support et les méthodes de diffusion**
3. **Identifier les acteurs impliqués**
4. **Identifier les types récits**

Ce document est un guide étape par étape destiné aux journalistes et aux chercheurs qui enquêtent sur la désinformation et les campagnes de dénigrement contre les médias. Il propose un canevas pour identifier les tactiques, techniques et procédures (TTPs) qui sous-tendent les campagnes de désinformation. Cette démarche vise à soutenir les efforts déployés pour exposer et contrer ces campagnes, de plus en plus utilisées pour cibler les médias critiques et miner la confiance du public envers des informations factuelles.

Ces règles de conduite ne sont pas **une panacée**, compte tenu du fait que la désinformation ne cesse d'évoluer avec les progrès technologiques. Il s'agit d'un **document dynamique** qui sera actualisé en fonction des nouvelles méthodologies développées.

1 Comprendre le contexte

L'objectif ici est de comprendre dans quelle mesure les campagnes de désinformation menées contre les médias reflètent des stratégies plus vastes visant à saper la confiance du public ou à promouvoir des récits spécifiques. Ce sont les principaux éléments que nous essayons généralement d'identifier :

Les événements et déclarations pertinents survenus durant la période de l'attaque

Identifier les évolutions ou événements de contexte plus larges qui ont contribué à créer un environnement dans lequel les journalistes sont ciblés pour leurs reportages. Il peut s'agir d'élections, de mouvements de protestation ou de crises ou troubles sociaux (par exemple, l'immigration, les problèmes sociaux).

Identifier la thématique spécifique ou le discours public qui semble avoir été à l'origine de l'attaque.

Identifier les discours de politiciens, de personnalités publiques influentes ou d'autres acteurs politiques qui ont créé un environnement légitimant les attaques contre les journalistes.

Contexte politique et social pertinent

Identifier les agendas des acteurs politiques ou autres acteurs concernés liés à la campagne de désinformation.

Les médias et les réseaux sociaux qui ont la réputation de diffuser des récits inexacts.

Consulter les plateformes en ligne, ainsi que les médias grand public pertinents et les médias marginaux ou « alternatifs ».

2 Analyser la chronologie, le support utilisé et les méthodes de diffusion

Les chercheurs et les journalistes doivent dresser une chronologie de l'attaque afin de mieux cerner le circuit de la campagne de désinformation. Ils devront en outre identifier les supports utilisés pour déployer la campagne, ainsi que les canaux utilisés pour optimiser sa diffusion, notamment les hashtags, les mèmes et les deepfakes vidéo/audio générés par l'intelligence artificielle.

Établir une chronologie de l'attaque : Identifier et décrire le(s) événement(s) clé(s) lié(s) aux attaques et créer une chronologie.

En premier lieu, interrogez la cible de la campagne pour avoir un premier rapport sur l'attaque. Les journalistes visés ont souvent une parfaite connaissance des aspects les plus importants des campagnes de désinformation et peuvent fournir un éclairage précieux sur le contexte, en aidant à établir une amorce de chronologie de la campagne. Si la cible était un média, interrogez les membres du personnel concernés : rédacteurs en chef, journalistes, community managers ou experts en sécurité numérique.

Relevez le reportage journalistique qui a été le déclencheur de la campagne de dénigrement contre le journaliste ou le média.

Noter quand et où (plateformes, sites web, etc.) les premières manifestations des attaques ont été détectées et les répertorier chronologiquement. Ce faisant, décrivez comment la campagne a été déployée sur les différentes plateformes pendant toute la durée de l'attaque.

Certains médias conservent des registres continus des attaques et du harcèlement, veillez donc à les vérifier et à inclure toutes les occurrences liées à l'attaque en cours enquête.

Identifier les canaux dattaques et d'harcèlement

Recherchez les pages et les profils qui mentionnent la cible dans les réseaux sociaux : Telegram, X, YouTube et Facebook (Meta) sont les plus utilisés (en date de 2024), mais examinez également Instagram, Threads, Reddit, TikTok, WhatsApp et d'autres plateformes en fonction de leur popularité dans le contexte local.

Les attaques et le harcèlement sont souvent menés par le biais de médias « marginaux », et de sites web usurpant l'identité de médias (voir section 3). Dans les cas où les informations sur ces plateformes ne sont pas claires, utilisez les données disponibles (registres officiels, données impressum), pour tenter de déterminer la propriété et le contexte éditorial.

Identifier les éléments qui ont été utilisés pour accélérer la diffusion de la campagne de dénigrement

Recherchez les hashtags, les mèmes, les images retouchées, les vidéos, les grossièretés, les informations personnelles, les deepfakes vidéo/audio sur différentes plateformes. Il faut garder à l'esprit que chaque publication n'est pas en soi une menace claire, et donc répertorier également les cas de menaces déguisées ou d'autres techniques d'intimidation telles que le Doxing (une partie des informations personnelles a été exposée, généralement l'email ou le numéro de téléphone du journaliste visé) afin d'obtenir une vue d'ensemble des récits.

Notez s'il existe des poursuites SLAPP (poursuite stratégique contre la mobilisation publique) ou des menaces de poursuites liées aux attaques.

Notez si le journaliste ou le média a récemment été la cible de cyberattaques.

Identifiez les communiqués de presse, les déclarations officielles et les apparitions dans les médias des acteurs politiques ou autres concernés.

BONNE PRATIQUE

Archiver les URL contenant tous les cas d'attaques ou de faux récits visant la cible.

Vous pouvez créer un système interne d'archivage ou utiliser des plateformes telles que https://ghostarchive.org/ ou https://archive.org/

3 Identifier les acteurs impliqués

À des fins d'enquête, il est essentiel d'identifier les acteurs qui ont instigué et/ou enclenché l'attaque, et ceux qui l'ont effectivement perpétrée. Il peut s'agir d'acteurs politiques, de groupes de discussion, de pages, de profils anonymes, de médias marginaux et de tout autre acteur pertinent associé à la campagne de désinformation.

Identifier et décrivez les acteurs les plus influents qui ont été à l'origine de la campagne de désinformation.

- Consigner une courte biographie, l'affiliation politique ou autre, les comptes de réseaux sociaux et les personnes qui les suivent, les déclarations pertinentes pour chaque acteur politique identifié.
- Recherchez les exemples où ces acteurs ont appelé leurs partisans à cibler le journaliste ou le média.

Identifier et décrire les plus pertinents (Alternatifs[1]) acteurs médiatiques qui ont rendu compte des attaques de manière positive et qui ont appuyé les récits désinformateurs.

- Vérifier les informations relatives au propriétaire du site web et la conformité du site avec les lois nationales.
- Noter la présence sur les réseaux sociaux, y compris les abonnés (followers).
- Vérifier Internet Archive (Wayback Machine) pour les versions antérieures du site web. Cela pourrait révéler des rubriques « à propos » qui étaient actives dans le passé, mais qui ont été supprimées par les administrateurs.
- Consultez les bases de données des médias, telles que Newsguard pour en savoir plus.

1 On entend par médias « alternatifs » les sites Internet qui se présentent comme des médias, mais qui opèrent en dehors de ce que l'on appelle le système médiatique dominant et qui, souvent, ne respectent pas les normes journalistiques professionnelles dans leur travail. Ils sont souvent dépourvus de transparence en termes de propriété et de structure éditoriale, les contributions qu'ils publient ne sont souvent pas signées et ils publient régulièrement des contenus manipulateurs et de la désinformation. Le but de leur travail n'est pas d'exercer le droit du public à accéder à des informations d'intérêt public, mais de monnayer des contenus sensationnalistes et/ou de promouvoir l'agenda de certains groupes d'intérêt.

BONNE PRATIQUE

Analyser l'infrastructure des principaux acteurs impliqués ainsi que les sites web. Cette analyse peut exiger une collaboration avec des spécialistes des technologies de l'information ou des experts OSINT et peut inclure, entre autres, les aspects suivants :

- Analyse DNS des sites de propagande
- Recherche inversée d'images de logos, d'icônes ou d'images pour les relier à d'autres publications
- Recherche de domaines et d'adresses IP

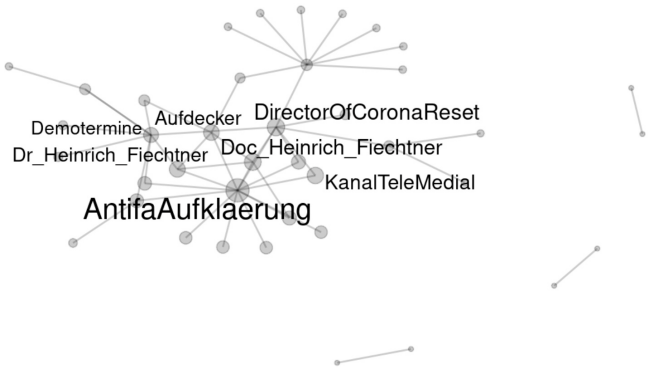
BONNE PRATIQUE

Effectuer une analyse des réseaux sociaux pour déterminer les liens, les acteurs et la manière dont ils sont connectés.

Plusieurs outils professionnels et des entreprises peuvent effectuer ce genre d'analyse, adaptée à vos besoins. Ils sont utiles pour identifier les acteurs qui ont échappé à la recherche initiale et peuvent montrer la diffusion de messages liés à des attaques. Voici une liste de logiciels avec lesquels nous avons travaillé :

- Gephi - The Open Graph Viz Platform
- NodeXL
- Gerulata
- Kivu.tech

Exemple : Découvrez le réseau de chaînes Telegram qui diffusaient des messages d'intimidation à l'encontre d'un journaliste allemand.



Cliquez ici pour lire le rapport complet.

4 Identifier les récits

L'identification du récit spécifique diffusé par la campagne de désinformation peut aider à révéler l'objectif de la campagne.

Vérifier les faits lors des attaques

Identifier et vérifier les faits (fact-check), les fausses informations utilisées dans l'attaque concernant un média et son appartenance politique, sa source de financement ou d'autres informations organisationnelles.

Être conscient que les campagnes de désinformation font sont parfois liésà des travaux antérieurs des journalistes qui ne sont pas strictement liés au travail journalistique de départ qui a été utilisé pour déclencher la campagne de dénigrement.

Identification des récits de désinformation

Faites une analyse de contenu des publications des réseaux sociaux et des articles des médias, ainsi que des discours publics.

Notez la terminologie et les expressions utilisées, faites attention aux néologismes.

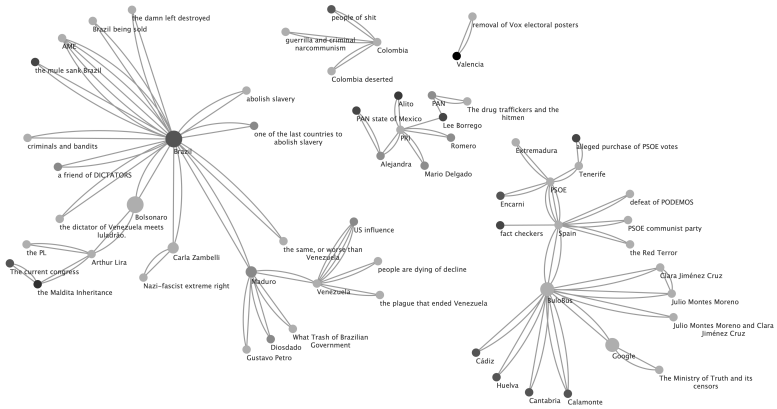
Utilisez le catalogue des récits de désinformation disponible sur la page de European Digital Media Observatory l'Observatoire européen des médias numériques (EDMO) (en Europe) et comparez vos résultats avec les récits de désinformation existants.

BONNE PRATIQUE

Créer des réseaux narratifs et traquer ces faux récits sur la durée. Ce type d'analyse offre un aperçu de la façon dont les récits contre les journalistes sont interconnectés et diffusés dans les mêmes canaux et au même moment, ce qui vous permet d'avoir une compréhension générale de la rhétorique générale.

La plupart des outils capables de réaliser des réseaux narratifs s'appuient sur l'IA. Veillez dans ce cas à respecter des principes de transparence sur l'utilisation de la technologie de l'IA dans la salle de rédaction. Il existe plusieurs directives, mais vous pouvez commencer par les principes de Partnership on AI que vous trouverez ici.

Exemple : En savoir plus sur les réseaux narratifs des théories du complot diffusées sur les canaux Telegram en Espagne.



Cliquez ici pour lire le rapport complet.

BONNE PRATIQUE

Faites un rapport sur cette enquête. En suivant ces directives, vous parviendrez à identifier les principaux éléments constitutifs d'une campagne de désinformation et à donner une réponse aux grandes questions journalistiques : Quoi ? Qui ? Pourquoi ? Comment ? Quand ? Où ?

Distribuez le rapport aux parties prenantes nationales et internationales concernées, telles que les associations de journalistes.

Avant de le faire, envisagez les risques juridiques éventuels (par exemple, adressez-vous aux associations journalistiques pour obtenir des conseils juridiques ou au service juridique de votre organe de presse). Étant donné que les reportages nommeraient probablement les personnes identifiées comme étant à l'origine des attaques, y a-t-il un risque que des personnes ou des entreprises intentent des poursuites pour diffamation ?

Autres ressources

Amnesty International: Le Citizen Evidence Lab

« Cet espace en ligne vise à aider les organisations de défense des droits de l'homme, les chercheurs, les enquêteurs, les étudiants, les journalistes et d'autres personnes à explorer et à partager des méthodes d'investigation numériques pour la recherche sur les droits de l'homme. »
Consultez la page ici.

Kit d'enquête en ligne de Bellingcat

« Ce kit d'investigation en ligne à code source ouvert comprend des conseils sur les services de satellite et de cartographie, des outils pour vérifier les photos et les vidéos, des sites web pour archiver les pages web, et bien d'autres choses encore. »
Consultez la page ici.

Digital Forensic Research Lab

« Le programme consiste en des ateliers et des sessions de formation pratique couvrant l'éducation aux médias, les techniques d'investigation en source ouverte, la vérification des faits et des sources, l'analyse narrative, la surveillance des réseaux sociaux, la géolocalisation, et bien d'autres sujets. »
Consultez leurs ressources et documents ici.

Observatoire européen des médias numériques (EDMO) : Formations

« L'EDMO propose régulièrement des modules de formation en ligne destinés à aider les différentes parties prenantes à comprendre et à combattre la désinformation en ligne. »
Consultez leur programme de formation ici.

Tactical Tech: Exposer l'invisible

« Exposer l'invisible se penche sur les différentes techniques, outils et méthodes, ainsi que sur les pratiques individuelles de ceux qui travaillent aux nouvelles frontières de l'investigation. »
Consultez la page ici.

Guide de vérification de la désinformation et de la manipulation des médias, par Craig Silverman

« Il fournit aux journalistes les connaissances nécessaires pour enquêter sur les comptes de réseaux sociaux, les bots, les applications de messagerie privée, les opérations d'information, les deep fakes, ainsi que sur d'autres formes de désinformation et de manipulation des médias. »
Télécharger le manuel ici.

Le projet

Decoding the disinformation playbook of populism in Europe

L'IPI, Taz et Faktograf travaillent ensemble pour décoder la propagande populiste en Europe en ciblant les fact-checkers et les journalistes d'investigation - qui sont tous deux des acteurs essentiels dans la lutte contre la désinformation.

European MEDIA AND INFORMATION Fund
Managed by Calouste Gulbenkian Foundation

Le projet **Decoding the disinformation playbook of populism in Europe** *est soutenu par le Fonds européen pour les médias et l'information, géré par la Fondation Calouste Gulbenkian.*

Guide élaboré par Tajana Broz (Faktograf) et Javier Luque Martínez (IPI).

In partnership with Canada

The translation of this resource was coordinated by the IPI Africa program, with the support of the Government of Canada's Office of Human Rights, Freedoms and Inclusion (OHRFI).