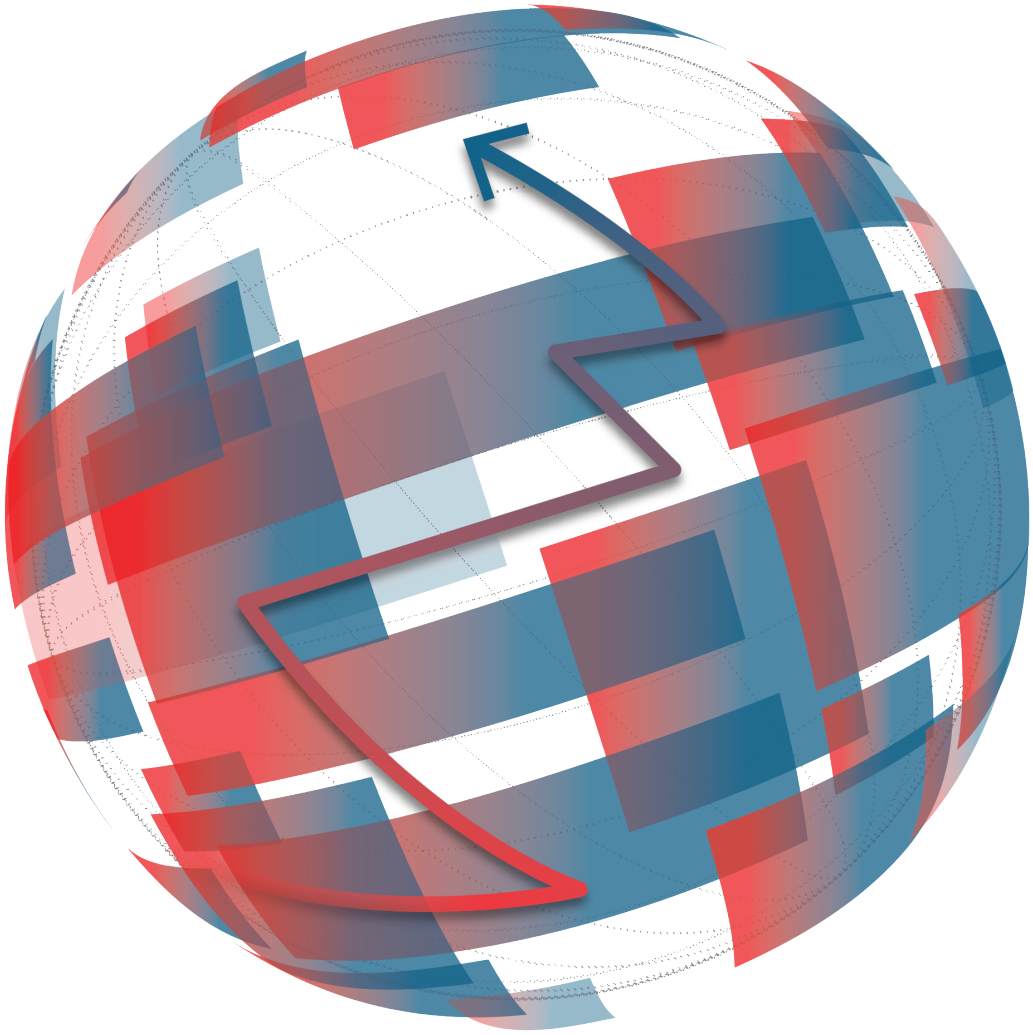


العنوان: دليل لفهم التضليل الإعلامي.

دليل خطوة بخطوة لتحديد المكونات الرئيسية للهجمات التضليلية التي تستهدف الصحفيين ووسائل الإعلام

دليل سريع

إليكم أربع خطوات أساسية يجب أن يتبعها الصحفيون والباحثون وغيرهم ممن يحققون في حملات التضليل ضد وسائل الإعلام:

1. **فهم السياق.**
2. **تحليل الجدول الزمني، والمنصات، وأساليب النشر.**
3. **تحديد الجهات الفاعلة المشاركة.**
4. **رصد السرديات المستخدمة.**

هذه الوثيقة عبارة عن دليل خطوة بخطوة موجه للصحفيين والباحثين المهتمين بالتحقيق في حملات التضليل والتشويه التي تستهدف وسائل الإعلام. يوفر الدليل إطارًا لتحديد التكتيكات والأساليب والإجراءات (TTPs) المستخدمة في حملات التضليل الإعلامي. يهدف هذا الإطار إلى دعم الجهود المبذولة لكشف هذه الحملات والتصدي لها، إذ تُستخدم بشكل متزايد لاستهداف وسائل الإعلام الناقدة وزعزعة ثقة الجمهور في الأخبار القائمة على الحقائق.

تجدر الإشارة إلى أن هذه الإرشادات ليست شاملة لكل الحالات، لأن أساليب التضليل الإعلامي تتطور باستمرار مع ظهور تقنيات جديدة. وعليه، تُعدّ هذه الوثيقة وثيقة حية يتم تحديثها باستمرار مع تطوير منهجيات جديدة.

1 فهم السياق.

الهدف هنا هو فهم ما إذا كانت الهجمات التضليلية على وسائل الإعلام وكيف تعكس استراتيجيات أوسع تهدف إلى تقويض الثقة العامة أو تعزيز سرديات معينة. فيما يلي العناصر الرئيسية التي نسعى عادةً إلى تحديدها:

الأحداث والتصريحات ذات الصلة خلال فترة الهجوم

- تحديد التطورات أو الأحداث الأوسع التي ساهمت في خلق بيئة يتم فيها استهداف الصحفيين بسبب تقاريرهم. قد تشمل هذه الأحداث الانتخابات، أو الحركات الاحتجاجية، أو الأزمات أو التحديات الاجتماعية (مثل قضايا الهجرة أو المشكلات الاجتماعية).
- تحديد الموضوع أو النقاش العام المحدد الذي يبدو أنه أثار الهجوم.
- تحديد التصريحات الصادرة عن السياسيين أو الشخصيات العامة المؤثرة أو غيرهم من الفاعلين السياسيين، والتي خلقت بيئة تُشرعن الهجمات ضد الصحفيين.

السياق السياسي والاجتماعي ذو الصلة

- تحديد أجندات الفاعلين السياسيين أو غيرهم من الأطراف ذات الصلة بحملة التضليل الإعلامي.

وسائل الإعلام والقنوات الاجتماعية التي تميل إلى نشر السرديات الكاذبة

- دراسة المنصات الإلكترونية، بالإضافة إلى وسائل الإعلام الرئيسية ذات التأثير الواسع والإعلام الهامشي أو «البديل».

2 تحليل الحدول الزمني والمنصات وأساليب النشر

ينبغي على الباحثين والصحفيين وضع حدول زمني للهحوم لفهم تطور حملة التضليل بشكل أفضل. بالإضافة إلى ذلك، يحب تحديد المنصات المستخدمة لنشر الحملة، وكذلك الوسائل التي ساهمت في تعزيز انتشارها، مثل الوسوم (الهاشتاغات)، الصور الساخرة (ميمز)، ومقاطع الفيديو أو الصوتيات المزيفة التي تم إنشاؤها بالذكاء الاصطناعي.

وضع حدول زمني للهحوم: تحديد ووصف الأحداث الرئيسية المرتبطة بالهحمات وإنشاء حدول زمني

- في المقام الأول، قم بإجراء مقابلة مع المستهدف من الحملة للحصول على رواية أولية عن الهحوم. غالبًا ما يكون لدى الصحفيين المستهدفين فهم حيد لأهم عناصر حملات التضليل ويمكنهم تقديم سياق قيّم يساعد في رسم حدول زمني أولي للحملة. إذا كان المستهدف مؤسسة إعلامية، تحدث إلى الموظفين المعنيين، مثل المحررين، الصحفيين، مديري المحتمعات الرقمية، أو خبراء الأمن الرقمي.
- لاحظ العمل الصحفي الذي استُخدم لإطلاق حملة التشويه ضد الصحفي أو المؤسسة الإعلامية.
- قم بتسحيل الوقت والمكان (المنصات، المواقع الإلكترونية، إلخ) حيث تم التعرف على أولى حالات الهحوم وقم بإدراحها ترتيبًا زمنيًا. وفي هذه العملية، قم بوصف كيفية نشر الحملة عبر المنصات خلال فترة استمرار الهحوم.
- بعض المؤسسات تحتفظ بسحلات مستمرة للهحمات والتحرش، لذا تأكد من التحقق منها وإدراج أي حالات مرتبطة بالهحوم قيد التحقيق.

تحديد قنوات الهحوم والتحرش

- ابحث في وسائل التواصل الاحتماعي عن الصفحات والحسابات التي تشير إلى المستهدف: تعد تليغرام، X (تويتر سابقًا)، يوتيوب وفيسبوك الأكثر شيوعًا (بحلول عام ٢٠٢٤)، ولكن لا تنسَ أيضًا البحث في إنستغرام، ثريدز، ريديت، تيك توك، واتساب وغيرها من المنصات وفقًا لشعبيتها في السياق المحلي.

غالبًا ما تُنفذ الهجمات والتحرشات عبر وسائل إعلام «هامشية» أو مواقع إلكترونية تنتحل صفة وسائل إعلام. (راجع القسم ٣). في الحالات التي لا يكون فيها خلفية هذه المنصات واضحة، استخدم البيانات المتاحة (السجلات الرسمية، بيانات «الإمبريسيوم») لمحاولة تحديد الملكية والخلفية التحريرية.

تحديد العناصر التي تم استخدامها لتسريع انتشار حملة التشويه

ابحث عن الوسوم (الهاشتاغات)، الصور الساخرة (ميمز)، الصور المعدلة، مقاطع الفيديو، الشتائم، المعلومات الشخصية، أو الفيديوهات/الصوتيات المزيفة عبر المنصات المختلفة. ضع في اعتبارك أن كل منشور فردي قد لا يشكل تهديدًا واضحًا، لذا قم أيضًا بتسجيل حالات التهديدات المبطنة أو غير المباشرة أو تقنيات الترهيب الأخرى مثل الكشف عن المعلومات الشخصية (دُكسينغ) (كأن يتم نشر البريد الإلكتروني أو رقم الهاتف الخاص بالصحفي المستهدف) للحصول على صورة شاملة عن السرديات المستخدمة.

لاحظ ما إذا كانت هناك دعاوى قضائية استراتيجية ضد المشاركة العامة (SLAPP) أو تهديدات برفع دعاوى مرتبطة بالهجمات.

لاحظ ما إذا كان الصحفي أو المؤسسة الإعلامية قد تعرض مؤخرًا لهجمات سيبرانية.

حدد البيانات الصحفية، والتصريحات الرسمية، والمظاهر الإعلامية للفاعلين السياسيين أو غيرهم من الجهات المعنية.

أفضل الممارسات

أفضل ممارسة: أرشفة الروابط الإلكترونية لجميع الحالات التي استُهدِف فيها الهدف

بهجمات أو روايات كاذبة. يمكنك إنشاء نظام داخلي للأرشفة أو استخدام منصات مثل https://ghostarchive.org/ أو archive.org/.

3 تحديد الجهات الفاعلة المشاركة

في سياق التحقيق، من الضروري تحديد الجهات الفاعلة التي كانت وراء التحريض على الهجوم أو التي قامت بإشعاله، بالإضافة إلى تلك التي نفذته على أرض الواقع. يمكن أن تشمل هذه الجهات فاعلين سياسيين، مجموعات دردشة، صفحات على الإنترنت، حسابات مجهولة الهوية، وسائل إعلام هامشية، أو أي أطراف أخرى مرتبطة بحملة التضليل.

تحديد ووصف الجهات الفاعلة الأكثر تأثيرًا التي كانت وراء حملة التضليل

- قم بتدوين سيرة ذاتية مختصرة لكل جهة فاعلة سياسية، بما في ذلك الانتماءات السياسية أو غيرها، حسابات وسائل التواصل الاجتماعي والمتابعين، وأي تصريحات ذات صلة.
- ابحث عن الحالات التي دعا فيها هؤلاء الفاعلون أتباعهم لاستهداف الصحفي أو المؤسسة الإعلامية.

تحديد ووصف الجهات الإعلامية (الهامشية)[1] الأكثر صلة التي كانت تواكب الهجوم وتدعم روايات التضليل

- تحقق من تفاصيل مالك الموقع ومدى امتثال الموقع للقوانين الوطنية.
- لاحظ حضورهم على وسائل التواصل الاجتماعي بما في ذلك عدد المتابعين.
- تحقق من أرشيف الإنترنت (آلة الزمن) لنسخ سابقة من الموقع. قد يكشف ذلك عن صفحات «من نحن» التي كانت نشطة في الماضي وتم حذفها لاحقًا من قبل المسؤولين.
- تحقق من قواعد بيانات الوسائط مثل Newsguard للحصول على مزيد من المعلومات

١ نعتبر وسائل الإعلام الهامشية تلك المواقع الإلكترونية التي تقدم نفسها كوسائل إعلام، ولكنها تعمل خارج ما يُعرف بالتيار الإعلامي السائد، وغالبًا ما لا تلتزم بالمعايير المهنية للصحافة في عملها. هذه المواقع غالبًا ما تكون غير شفافة من حيث الملكية والتركيب التحريري، والمساهمات التي تنشرها غالبًا ما تكون بدون توقيع، كما أنها تنشر بانتظام محتوى تحريفيًا ومضللًا. الغرض من عملها ليس ممارسة حق الجمهور في الوصول إلى المعلومات ذات المصلحة العامة، بل تحقيق أرباح من المحتوى الاستفزازي و/أو الترويج لأجندات مجموعات مصالح معينة.

أفضل الممارسات

إحراء تحليل للبنية التحتية للجهات الفاعلة الرئيسية المشاركة وكذلك المواقع الإلكترونية. قد يتطلب هذا التعاون مع موظفي تكنولوجيا المعلومات أو خبراء الاستخبارات المفتوحة (OSINT) ويمكن أن يشمل، من بين أمور أخرى:

- تحليل نظام أسماء النطاقات (DNS) لمواقع الدعاية
- البحث العكسي للصور الخاصة بالشعارات أو الرموز أو الصور لتتبعها إلى منشورات أخرى
- البحث عن اسم النطاق (Domain) وعنوان الـ IP

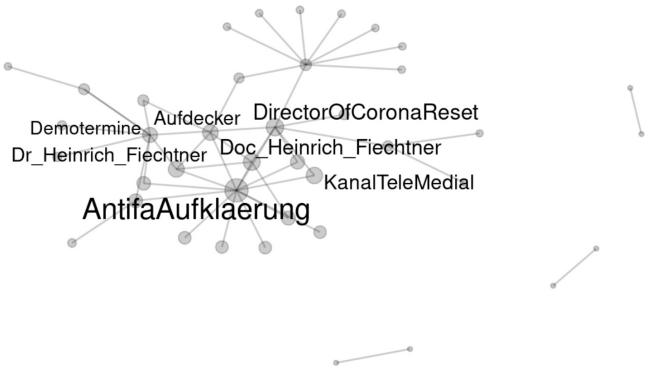
أفضل الممارسات

إحراء تحليل لشبكة التواصل الاجتماعي لاكتشاف الروابط والجهات الفاعلة وكيفيةة تواصلها

يمكن للعديد من الأدوات والشركات المتخصصة إحراء هذا النوع من التحليل، حسب احتياجاتك. هذه الأدوات مفيدة في تحديد الجهات الفاعلة التي قد تكون قد فاتت خلال البحث الأساسي، ويمكن أن تظهر انتشار الرسائل المرتبطة بالهجمات. إليك قائمة بالبرمجيات التي استخدمناها:

- Gephi - منصة التصور البياني المفتوحة
- NodeXL
- Gerulata
- Kivu.tech

مثال: تعرف على المزيد حول شبكة القنوات في تليغرام التي كانت تشارك رسائل تهديدية ضد صحفي محلي في ألمانيا.



انقر هنا لقراءة التقرير الكامل.

4 تحديد الروايات

إن تحديد الرواية المحددة التي يتم نشرها من خلال هجوم التضليل يمكن أن يساعد في الكشف عن الهدف وراء الحملة.

التحقق من صحة الادعاءات التي تم طرحها أثناء الهجمات

- تحديد والتحقق من صحة المعلومات المضللة المستخدمة في الهجوم حول وسيلة الإعلام وميولها السياسية، تمويلها، أو أي معلومات تنظيمية أخرى.
- كن على دراية بأن حملات التضليل أحيانًا تشير إلى أعمال سابقة للصحفيين التي قد لا تكون مرتبطة بشكل مباشر بالعمل الصحفي الأصلي الذي استخدم لإشعال حملة التشهير.

تحديد روايات التضليل

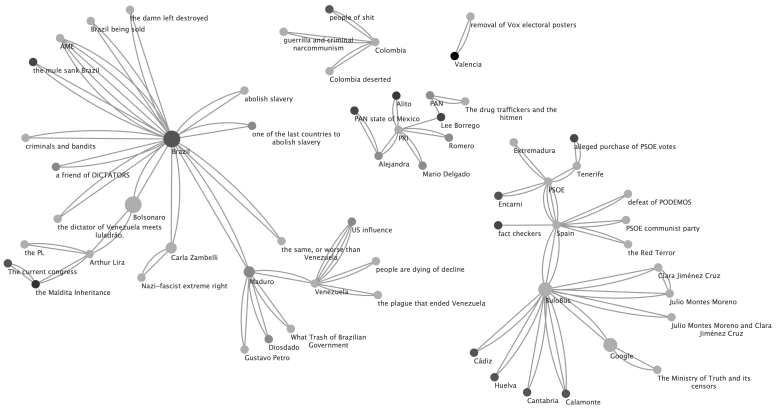
- إجراء تحليل للمحتوى المنشور على وسائل التواصل الاجتماعي والمقالات الإعلامية والخطب العامة.
- لاحظ العبارات والكلمات المستخدمة، واهتم بالكلمات الحديدة (النيوولوجيزمات).
- استخدم فهرس روايات التضليل المتاح على صفحة «المراقبة الرقمية للإعلام الأوروبي» (EDMO) في أوروبا، وارتبط استنتاجاتك مع الروايات التضليلية الموجودة.

أفضل الممارسات

إنشاء شبكات الروايات وتتبع هذه الروايات المضللة عبر الزمن. يقدم هذا النوع من التحليل لمحة عامة عن كيفية ارتباط وتوزيع الروايات ضد الصحفيين في نفس القنوات وفي نفس الوقت، مما يمنحك فهماً شاملاً للخطاب الأوسع.

تعتمد معظم الأدوات التي يمكنها إجراء تحليلات شبكات الروايات على الذكاء الاصطناعي. في هذه الحالة، تأكد من أنك تتبع مبادئ الشفافية في استخدام تقنيات الذكاء الاصطناعي في غرفة الأخبار. هناك العديد من الإرشادات التي يمكنك البدء بها، ولكن يمكنك البدء بمبادئ الشراكة في الذكاء الاصطناعي التي يمكنك العثور عليها هنا.

مثال: تعرف على المزيد حول شبكات الروايات المتعلقة بنظريات المؤامرة التي تم نشرها عبر قنوات تليغرام في إسبانيا.



انقر هنا لقراءة التقرير الكامل.

أفضل الممارسات

إعداد تقرير عن هذه التحقيقات. باتباع هذه الإرشادات، ستكون قادرًا على تحديد المكونات الرئيسية التي تشكل حملة التضليل الإعلامي وتقديم إجابات على الأسئلة الصحفية الرئيسية: ماذا؟ من؟ لماذا؟ كيف؟ متى؟ أين؟

وزع التقرير على الأطراف المعنية الوطنية والدولية مثل الجمعيات الصحفية

قبل القيام بذلك، ضع في اعتبارك أي مخاطر قانونية (مثل: التحدث مع الجمعيات الصحفية للحصول على استشارات قانونية أو مع القسم القانوني في وسيلة الإعلام الخاصة بك). نظرًا لأن التقارير من المحتمل أن تذكر أولئك الذين تم التعرف عليهم كمخططين للهجمات، هل هناك فرصة أن يقوم أفراد أو شركات برفع دعاوى تشهير؟

الموارد الأخرى

Amnesty International: Citizen Evidence Lab

"تسعى هذه المساحة على الإنترنت لدعم المنظمات الحقوقية، الباحثين، المحققين، الطلاب، الصحفيين وغيرهم لاستكشاف ومشاركة أساليب التحقيق الرقمي في أبحاث حقوق الإنسان."
زور الصفحة هنا.

Bellingcat›s Online Investigation Toolkit

"يتضمن هذا الدليل المفتوح المصدر لأدوات التحقيق عبر الإنترنت إرشادات حول خدمات الأقمار الصناعية والملاحة، أدوات للتحقق من الصور والفيديوهات، مواقع لحفظ صفحات الويب، وأكثر من ذلك."
زور المواد هنا.

Digital Forensic Research Lab

"يتكون البرنامج من ورش عمل وحلسات تدريب عملية تغطي محو الأمية الإعلامية، تقنيات التحقيق المفتوحة المصدر، التحقق من الحقائق والتحقق من المصادر، تحليل الروايات، مراقبة وسائل التواصل الاحتماعي، الحغرافيا المكانية، والعديد من المواضيع الأخرى."
زور الموارد والمواد هنا.

European Digital Media Observatory (EDMO): Trainings

"تقدم EDMO وحدات تدريبية عبر الإنترنت بشكل دوري لدعم أصحاب المصلحة المختلفين في فهم ومكافحة المعلومات المضللة عبر الإنترنت."
زور برنامج التدريب هنا.

Tactical Tech: Exposing the Invisible

"يستعرض Exposing the Invisible تقنيات وأدوات وأساليب مختلفة حنبًا إلى حنب مع الممارسات الفردية لأولئك الذين يعملون في واحهات التحقيقات الحديثة."
زور الصفحة هنا.

Verification Handbook for Disinformation and Media Manipulation, by Craig Silverman

"يُزود هذا الكتاب الصحفيين بالمعرفة اللازمة للتحقيق في حسابات وسائل التواصل الاحتماعي، الروبوتات، تطبيقات المراسلة الخاصة، العمليات الإعلامية، والتزييف العميق، فضلاً عن أشكال أخرى من المعلومات المضللة والتلاعب الإعلامي."
حمّل الدليل هنا.

المشروع:

فك شفرة دليل المعلومات المضللة للشعبوية في أوروبا

تتعاون كل من IPI، Taz، وFaktograf للعمل معًا لفك شفرة دعاية الشعبوية في أوروبا التي تستهدف المدققين في الحقائق والصحفيين الاستقصائيين – الذين يشكلون لاعبين أساسيين في مكافحة المعلومات المضللة.

European MEDIA AND INFORMATION Fund

Managed by
Calouste Gulbenkian Foundation

يتم دعم مشروع «فك شفرة دليل المعلومات المضللة للشعبوية في أوروبا» من قبل صندوق الإعلام والمعلومات الأوروبي، الذي تديره مؤسسة كالوس غولبنكين.

إخلاء المسؤولية:
المسؤولية الكاملة عن أي محتوى مدعوم من صندوق الإعلام والمعلومات الأوروبي تقع على عاتق المؤلف (المؤلفين) وقد لا يعكس بالضرورة مواقف EMIF والشركاء في الصندوق، مؤسسة كالوس غولبنكين والمعهد الأوروبي للحامعة.

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).