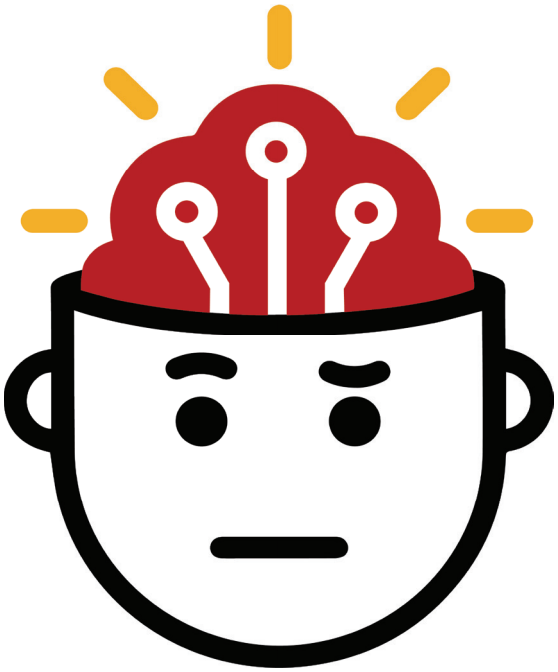


کتابچه راهنمای راستی‌آزمایی

برای دیس‌اینفورمیشن و دستکاری‌های رسانه‌ای

راهنمای جامع برای پلتفرم‌های تحقیقاتی و حساب‌های آنلاین در مسیر آشکار کردن
فعالیت‌های غیرمعتبر و محتوای دستکاری‌شده

گردآوری و تدوین: کرگ سیلورمن

European Journalism Centre
DataJournalism.com
Craig Newmark Philanthropies
فکت‌نامه Factnameh

فصل‌ها

تحقیق درباره‌ی اطلاعات نادرست و دستکاری اطلاعات در رسانه‌ها

تدوین و گردآوری: کرگ سیلورمن

کرگ سیلورمن سردبیر سایت خبری بازفید (BuzzFedd) است و رهبری این وب‌سایت را که اخبار جهانی مربوط به پلتفرم‌ها، اطلاعات نادرست در فضای مجازی و گمراه‌سازی‌های رسانه‌ای را پوشش می‌دهد، بر عهده دارد. او پیش از این کتابچه‌ی راهنمای راستی‌آزمایی و همچنین کتابچه‌ی راهنمای راستی‌آزمایی در روزنامه‌نگاری تحقیقی را گردآوری و ویرایش کرده و مؤلف کتاب دروغ‌ها، دروغ‌های لعنتی و محتوای وایرال شده: چگونه وب‌سایت‌های خبری شایعات، ادعاهای بی‌اساس و اطلاعات نادرست را در فضای مجازی پراکنده (و یا بی‌اعتبار) می‌کنند نیز هست.

در دسامبر ۲۰۱۹، یکی از کاربران توئیتر با نام کاربری NickCiarelli@ ویدئوی رقص کوتاهی را به اشتراک گذاشت که به گفته‌ی او توسط حامیان کمپین انتخاباتی مایکل بلومبرگ نامزد انتخابات ریاست جمهوری اجرا شده بود.

طراحی رقص و شوروشوق ساختگی و ملال‌آور ویدئو باعث شد این توئیت بارها، عمدتا توسط کسانی که از تمسخر آن لذت می‌بردند، ریتوییت و لایک شود. در نهایت، این ویدئو بیش از پنج‌میلیون بار در توئیتر دیده شد.

بیوگرافی سیارلی در حساب توئیترش می‌گوید که او در کمپین بلومبرگ کارآموز بوده و توئیت‌های بعدی او حاوی نکاتی در اثبات این ادعا است؛ به‌عنوان مثال اسکرین‌شاتی از ایمیل یکی از کارکنان کمپین بلومبرگ که بودجه‌ی ساخت این ویدئو را تأیید می‌کند.

اما با جستجوی کوتاهی در گوگل مشخص شد سیارلی درواقع یک کمدین است که در گذشته ویدئوهای طنز ساخته است. و ایمیلی که از طرف کارمند ستاد بلومبرگ ارسال شده بود؟ با جستجوی کوتاه دیگری در گوگل مشخص شد فرستنده‌ی ویدئو برَد اِونز، کمدین و همکار سیارلی در برنامه‌های طنزش، بوده است. تمام این اطلاعات با یک جستجوی ساده و کوتاه در گوگل قابل دسترسی بود.

اما در دقایق و ساعت‌های اولیه پس از انتشار آن ویدئوی خجالت‌آور عده‌ای باور کردند که ویدئو واقعا محصول کمپین تبلیغاتی بلومبرگ بوده است.

مگی هابرمن، خبرنگار سیاسی برجسته‌ی نیویورک تایمز، در توئیتی نوشت که خبرنگارانی که کارزارها پیشین بلومبرگ در انتخابات شهرداری را پوشش می‌دادند، دلایلی داشتند که باعث می‌شد فورا آن ویدئو را به‌عنوان طنز را رد نکنند:

دانش می‌تواند اشکال مختلفی داشته باشد، و در محیط دیجیتال جدید روزنامه‌نگاران باید از اتکای بیش‌از حد به هرگونه منبع اطلاعاتی حذر کنند –حتی اگر این منبع تجربه‌ی دست‌اول خودشان باشد.

از قرار معلوم، برخی از خبرنگارانی که بلومبرگ و سبک مبارزات انتخاباتی او را می‌شناختند، احساس کردند که این ویدئو می‌تواند واقعی باشد، درحالیکه کسانی که هیچ‌چیز در مورد بلومبرگ نمی‌دانستند و بنابراین باید ویدئو را بر اساس منبع به‌اشتراک‌گذاری‌اش قضاوت می‌کردند، می‌توانستند بلافاصله به جواب صحیح دست پیدا کنند –در این مورد، با جستجوی ساده‌ی نام فردی که ویدئو را به اشتراک گذاشته بود در گوگل.

نکته این نیست که تجربه‌ی پوشش خبری کارزارهای انتخاباتی بلومبرگ تجربه‌ی بدی است. نکته این است که هر آن این احتمال وجود دارد چیزهایی که فکر می‌کنیم می‌دانیم، گمراهمان کنند. و در برخی موارد، دانش پایه و تجربه می‌تواند حتی منفی باشد. این احتمال نیز وجود دارد که نشانه‌های دیجیتالی، مانند ریتوییت‌ها و تعداد دفعات بازدید و یا تلاش‌هایی که برای دستکاری آن‌ها صورت می‌گیرد، ما را فریب دهد.

همانطور که ویدئوی بلومبرگ نشان داد، ایجاد سیگنال‌های گمراه‌کننده‌ای مانند بیوگرافی توئیتر یا اسکرین‌شاتی از یک ایمیل که به نظر می‌رسد ادعای مورد نظر را اثبات می‌کند، کار چندان دشواری نیست. این‌ها به‌نوبه‌ی خود به پربازدید شدن محتوا کمک می‌کنند. و هرچه تعداد بازتوییت‌ها و لایک‌ها بیشتر شود، این سیگنال‌ها عده‌ی بیشتری را قانع خواهند کرد که ویدئو واقعی است.

البته نمونه‌های فریب‌کارانه‌تر و پیچیده‌تر از نمونه‌ی حاضر هم بسیارند. برخلاف سیارلی، افرادی که کمپین‌های دیس‌اینفورمیشن و عملیات اطلاعاتی را راه‌اندازی می‌کنند به‌ندرت دست خود را رو می‌کنند. اما این مطالعه‌ی موردی نشان می‌دهد پیدا کردن مسیر درست در این محیط اطلاعاتی مملو از سیگنال‌های ساختگی کیفیت و اطمینان، تا چه‌اندازه می‌تواند برای همه، از جمله برای روزنامه‌نگاران، گیج‌کننده و دشوار باشد.

اعتماد اساس جامعه و عنصری است که تعاملات را راحت و روان می‌کند و کلید روابط انسانی است. اما فعالیت با پیش‌فرض اعتماد در محیط دیجیتال خطرناک است.

اگر پیش‌فرض شما این باشد که حساب‌های کاربری‌ای که ویدئویی را در فضای توئیتر بازنشر می‌کنند، این کار را به طور طبیعی انجام می‌دهند، بازی خواهید خورد. اگر بر این باور باشید که نظراتی که در مورد یک محصول ثبت شده همه از طرف مصرف‌کنندگان واقعی است، پولتان را دور خواهید ریخت. اگر باور داشته باشید که هر مقاله‌ای که در فید خبری خود می‌بینید، مجموعه‌ای بی‌طرفانه از مهم‌ترین چیزهایی است که باید ببینید، درنهایت اطلاعات نادرست خواهید داشت.

درک این واقعیت برای همه مهم، اما برای روزنامه‌نگاران حیاتی است. ما هدف کمپین‌هایی قرار می‌گیریم که به‌خوبی و با بودجه‌ی کافی به‌گونه‌ای هماهنگ شده‌اند که توجه ما را به خود جلب کنند، طوری فریبمان دهند که پیام‌ها را پراکنده کنیم و ما را مقهور اراده‌ی دولت‌ها و سایر منابع بزرگ قدرت کنند.

خبر خوب این است که این یک فرصت –و یک ضرورت– برای بررسی و پژوهش نیز ایجاد می‌کند.

این کتابچه از دانش و تجربه‌ی روزنامه‌نگاران و پژوهش‌گران برتر استفاده می‌کند تا راهنمایی‌هایی در مورد چگونگی انجام تحقیقات در مورد دستکاری اطلاعات، اطلاعات نادرست و عملیات اطلاعاتی در رسانه‌های دیجیتال ارائه دهد.

ما در یک اکوسیستم اطلاعاتی پیچیده و به‌سرعت‌دگرگون‌شونده فعالیت می‌کنیم. کار در این اکوسیستم مستلزم در پیش گرفتن رویکردی به همان اندازه منعطف و متغیر است؛ رویکردی که بر اساس آزمایش مفروضاتمان، ردیابی و پیش‌بینی مخالفان و حریفان، استفاده از بهترین روش‌های تحقیق منبع‌باز و تکنیک‌های گزارش‌دهی سنتی بنا شده باشد. آسیب‌پذیری دنیای دیجیتال و داده‌محورْ ما روزنامه‌نگاران را ملزم می‌کند که تمامی جنبه‌های آن را مورد مداقه و بررسی قرار دهیم و مهارت‌هایمان را برای راهنمایی مردم به سمت اطلاعات دقیق و قابل‌اطمینان ببریم. ما روزنامه‌نگاران باید به این موضوع نیز بیندیشیم که چگونه ممکن است ناخواسته هیزم به آتش عاملان بد و کمپین‌هایی بریزیم که برای سودجویی از ما طراحی شده‌اند و چگونه ممکن است بدون در دسترس داشتن شواهد کافی، عجولانه انگشت اتهام را به سمت عاملان دولتی بگیریم.

هدف کتابچه‌ی راهنمای حاضر تجهیز روزنامه‌نگاران به مهارت‌ها و تکنیک‌های لازم برای انجام مؤثر و مسئولانه‌ی این وظیفه است. این کتابچه همچنین دانش پایه، زمینه‌ی لازم و ذهنیت مورد نیازی را ارائه می‌کند که روزنامه‌نگاران را قادر خواهد ساخت کارهایی با کیفیت بالا برای آگاه کردن عموم ارائه دهند، دست عاملان بد را رو کنند و به بهبود محیط اطلاعاتی‌مان کمک کنند. اما اولین چیزی که باید به خاطر داشته باشیم این است که دانش و ابزارهای عملی، بدون داشتن ذهنیت و طرز فکر درست سودی نخواهند داشت.

این به معنای درک این نکته است که در محیط دیجیتال همه چیز می‌تواند بازی و فریبکاری باشد و باید بتوانیم افراد و نهادهایی را که انگیزه‌ی لازم برای انجام چنین کارهایی را دارند شناسایی کنیم. زیبایی محیط دیجیتال این است که اغلب- اگرچه، نه همیشه- در آن دنباله‌ای از داده‌ها، تعاملات، ارتباطات و سایر نشانه‌های کوچک دیجیتال وجود دارد که می‌توان دنبالشان کرد. و اگر بدانید کجا و چگونه جستجو کنید، بخش عمده‌ای از این اطلاعات را می‌توان در فضای عمومی یافت.

بررسی فضای دیجیتال یعنی نباید ظاهر هیچ‌چیز را باور کنیم. یعنی باید درک کنیم اطلاعاتی که در ظاهر کمّی و مبتنی بر داده هستند –تعداد لایک‌ها، اشتراک‌گذاری‌ها، ریتوییت‌ها، ترافیک، نظرات کاربران درباره‌ی یک محصول، تعداد کلیک‌های تبلیغاتی–غلب و به‌راحتی دستکاری می‌شوند؛ یعنی درک این نکته که خبرنگاران هم هدف اصلی گمراه‌سازی‌های رسانه‌ای و عملیات اطلاعاتی– چه به‌عنوان طعمه و چه به‌عنوان هدف حمله– هستند و هم مجاری کلیدی برای انتشار اطلاعات نادرست و دروغ‌پراکنی به شمار می‌روند. و این یعنی باید خود و همکارانتان را به ذهنیت، تکنیک‌ها و ابزار لازم مجهز کنید تا مطمئن شوید اطلاعات قابل‌اطمینان و دقیقی در اختیار عموم قرار می‌دهید و دروغ‌ها، محتوای دستکاری‌شده و کمپین‌های اوباش مجازی (ترول‌ها) را بازنشر نمی‌کنید.

در مرکز این ذهنیت، پارادوکس تحقیقات دیجیتال قرار دارد: ابتدابه‌ساکن با اعتماد نکردن به هیچ‌چیز کارمان را شروع می‌کنیم و کاری که خواهیم کرد به ما نشان خواهد داد به چه چیز باید اطمینان کنیم و به چه چیزی نه. و این به ما کمک می‌کند محصول کارمان چیزی باشد که جوامعی که به آن‌ها خدمت می‌کنیم مایل باشند و بتوانند به آن اطمینان کنند.

علاوه بر این برخی اصول پایه‌ای وجود دارند که به کرات در فصول و مطالعات موردی روی آن‌ها تاکید شده‌اند:

- **مثل رقیب فکر کنید.** هر ویژگی و کارکرد جدید یک پلتفرم یا سرویس دیجیتال می‌تواند به نحوی مورد سوء استفاده قرار بگیرد. بسیار مهم است که خود را به جای کسی قرار دهید که به دلایل ایدئولوژیک، سیاسی، مالی و غیره به دنبال دستکاری محیط دیجیتال است. وقتی به محتوا و پیام‌های دیجیتال نگاه می‌کنید، باید انگیزه‌های ایجاد و انتشارشان را در نظر بگیرید. همچنین، ضروری است که از آخرین تکنیک‌های مورد استفاده‌ی عاملان بد، بازاریاب‌های دیجیتال و دیگرانی که معیشتشان به یافتن راه‌های جدید برای جلب توجه و کسب درآمد از محیط دیجیتالی متکی است، مطلع باشید.

- **روی عاملان، محتوا، رفتار و شبکه‌ها تمرکز کنید.** هدف این است که عاملان، محتوا و رفتار را تجزیه و تحلیل کنیم و ببینیم چگونه می‌توان فعالیت یکپارچه‌ی آن‌ها را به‌صورت شبکه مستند کرد. با مقایسه و مقابله‌ی این چهار عامل با یکدیگر کم‌کم خواهید توانست آنچه را که می‌بینید درک کنید. همانطور که در فصل‌های پیش رو و مطالعات موردی خواهید دید، در بسیاری مواقع رویکرد اساسی این است که با یک محتوا یا موجودیتی مثل یک وب‌سایت، شروع می‌کنید و با اتکا بر آن شبکه‌ی بزرگ‌تر را از طریق الگوی رفتار و سایر ارتباطات شناسایی می‌کنید. این می‌تواند شامل بررسی محتوا و عاملان در پلتفرم‌های مختلف و گاهی به زبان‌های گوناگون باشد.

- **رصد و جمع‌آوری کنید.** بهترین راه برای شناسایی دستکاری در رسانه‌ها و اطلاعات نادرست این است که همیشه گوش به زنگ باشید. رصد و ردیابی مداوم عاملان شناخته‌شده و موضوعات و اجتماع‌های مرتبط با آن‌ها ضروری است. آنچه می‌توانید، از صفحات گسترده گرفته تا پوشه‌های حاوی اسکرین‌شات یا محتوایی که با استفاده از ابزارهای پولی مانند Hunchly به دست آورده‌اید، را حفظ و سازماندهی کنید.

- **در نسبت دادن اعمال به اشخاص و نهادها دقت کنید.** گاهی اوقات تعیین اینکه دقیقا چه کسی پشت یک حساب کاربری خاص، یک محتوا یا یک عملیات اطلاعاتی بزرگ‌تر است ممکن نیست. یکی از دلایل این است که عاملانی با انگیزه‌های متفاوت می‌توانند به شیوه‌های مشابهی رفتار کنند و محتوای مشابهی را تولید یا تقویت کنند. حتی خود پلتفرم‌ها -که منابع بیشتر و دسترسی بهتری به داده‌ها دارند- نیز گاهی در نسبت دادن عملیات به فرد یا نهادی خاص اشتباه می‌کنند. موفق‌ترین و قانع‌کننده‌ترین شواهد معمولا آن‌هایی هستند که شواهد دیجیتال را با اطلاعاتی از منابع داخلی ترکیب می‌کنند -ترکیبی ایده‌آل از کار تحقیقاتی آنلاین و سنتی. اگرچه، با تکامل دانش افراد و نهادهای دولتی و پیدا شدن راه‌های جدید برای پنهان کردن اثرانگشت اینترنتی این کار از پیش نیز دشوارتر شده است. انتساب، کار دشواری است و خطا در انتساب می‌تواند تمام کار دقیقی را که تا آن مرحله صورت گرفته، زیر سؤال ببرد و بی‌اعتبار کند.

و درنهایت، نکته‌ای در خصوص دو کتابچه‌ی راهنمای دیگری که پیش از نسخه‌ی حاضر تهیه شده بودند. این اثر از مفاهیم پایه‌ی کتابچه‌ی راهنمای راستی‌آزمایی و کتابچه‌ی راهنمای راستی‌آزمایی در گزارش‌های تحقیقی سود می‌جوید. هر کدام از این کتاب‌ها مهارت‌های اساسی برای رصد رسانه‌های اجتماعی، راستی‌آزمایی تصاویر، ویدئوها، حساب‌های کاربری در رسانه‌های اجتماعی و استفاده از موتورهای جستجو برای شناسایی افراد، شرکت‌ها و سایر نهادها ارائه می‌دهند.

بسیاری از فصول و مطالعات موردی در این کتاب راهنما با این فرض نوشته شده‌اند که خوانندگان دانش اولیه مندرج در نسخ قبلی، به ویژه اولین کتابچه‌ی راهنما، را دارند. اگر دنبال کردن مطالب این کتابچه برایتان دشوار است، توصیه‌ی ما این است که با اولین کتابچه‌ی راهنما شروع کنید.

بسیار خوب، پس شروع کنیم.

عصر آشفتگی اطلاعات

نوشته‌ی: کلر واردل

کلر واردل مسئول هدایت استراتژیک و تحقیقات در مؤسسه‌ی فِرْست درفت است، یک سازمان غیرانتفاعی بین‌المللی که کارش پشتیبانی از روزنامه‌نگاران، دانشگاهیان و فناورانی است که برای مقابله با چالش‌های مربوط به اعتماد و حقیقت در عصر دیجیتال تلاش می‌کنند. او عضو مرکز شورنستاین برای رسانه، سیاست و سیاست‌گذاری عمومی در دانشکده‌ی کندی هاروارد، مدیر تحقیقات در مرکز تُوْ برای تحصیلات تکمیلی روزنامه‌نگاری در دانشگاه کلمبیا و رئیس بخش رسانه‌های اجتماعی در کمیساریای عالی سازمان ملل متحد برای پناهندگان است.

همه می‌دانیم که دروغ، شایعه و پروپاگاندا مفاهیم جدیدی نیستند. انسان‌ها همیشه توانایی فریبکار بودن را داشته‌اند و نمونه‌های تاریخی چشمگیری وجود دارد که نشان می‌دهد چگونه از محتوای ساختگی برای گمراه کردن مردم، بی‌ثبات کردن دولت‌ها یا بالا بردن ارزش بازارهای سهام استفاده می‌شد. آنچه در عصر ما جدید است سهولت ایجاد محتوای نادرست و گمراه‌کننده‌ای که قانع‌کننده و باورپذیر می‌نماید و نیز سرعت پراکنده شدن این اطلاعات در جهان است.

این را نیز می‌دانیم که فریبکاری پیچیدگی‌های خاص خودش را دارد و نمی‌توان همه‌ی فریبکاران را به یک چوب راند. به‌عنوان مثال، دروغ مصلحتی‌ای که برای خاموش کردن آتش نزاع خانوادگی گفته می‌شود با اظهارات گمراه‌کننده‌ی یک سیاستمدار که هدفش جذب رأی‌دهندگان بیشتر است یکی نیست. یک کمپین تبلیغاتی تحت حمایت دولت با تئوری توطئه درباره فرود بر ماه یکسان نیست.

متاسفانه، در چند سال گذشته هر چیزی که ممکن است در دسته‌بندی‌های توضیح داده شده در این کتابچه بگنجد، «اخبار جعلی» (Fake News) نامیده شده؛ یک اصطلاح ساده که مقبولیت جهانی پیدا کرده و اغلب نیازی به ترجمه‌ی آن نیز حس نمی‌شود. دلیل استفاده‌ام از قید متأسفانه این است که این اصطلاح برای توصیف پیچیدگی‌ای که با آن روبرو هستیم کافی نیست. در مورد بیشتر محتواهای

گمراه‌کننده حتی تلاشی برای قبولاندن آن محتوا به‌عنوان خبر نیز صورت نمی‌گیرد. این مطالب در قالب میم‌ها، ویدئوها، تصاویر و یا فعالیت‌های هماهنگ‌شده در توئیتر، یوتیوب، فیس‌بوک یا اینستاگرام ارائه می‌شوند. و البته بیشتر آن‌ها کاملا جعلی و دروغین نیستند. این مطالب در اغلب مواقع واقعی و بعضا گمراه‌کننده هستند، اما مشکل اصلی اینجا است که خارج از زمینه و بستر واقعی و خاص خود استفاده می‌شوند.

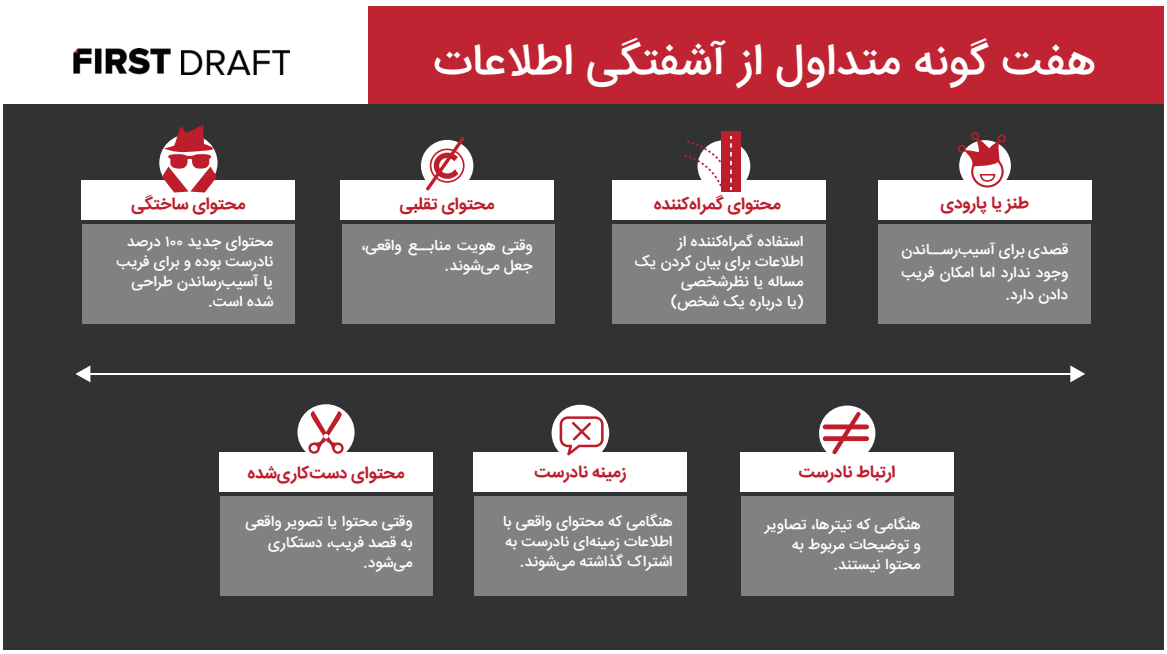
تأثیرگذارترین نوع اطلاعات نادرست مطالبی هستند که ذره‌ای از حقیقت در آنها نهفته است: زدن برچسب نادرست به یک محتوای درست، یا به اشتراک گذاشتن چیزی به عنوان یک محتوای جدید در حالی که درواقع سه سال از عمرش می‌گذرد.

شاید بغرنج‌ترین بخش مشکل این باشد که اصطلاح «اخبار جعلی» تبدیل به سلاحی شده است که سیاستمداران و حامیانشان از آن برای حمله به رسانه‌های خبری حرفه‌ای در سراسر جهان استفاده می‌کنند.

ناامیدی من از کارایی این اصطلاح باعث شد با کمک همکارم، حسین درخشان، اصطلاح «اختلال اطلاعاتی» را به جای آن ضرب کنم. در سال ۲۰۱۷ و در گزارشی با عنوان «آشفتگی اطلاعات»، به بررسی چالش‌های مرتبط با اصطلاحات و واژگان فنی این حوزه پرداختیم. در این فصل، برخی از دلایل اهمیت کلیدی تبیین و تعریف صحیح اصطلاحات در درک موضوعات این حوزه و همچنین بحث انتقادی در خصوص آن را توضیح خواهم داد.

۷ نوع آشفتگی اطلاعات

در سال ۲۰۱۷، گونه‌شناسی زیر را برای روشن کردن انواع مختلف آشفتگی اطلاعات ارائه دادم:



طنز/نقیض

قابل درک است که چرا بسیاری افراد از اینکه من طنز را در این گونه‌شناسی گنجانده‌ام انتقاد کرده‌اند و خود من نیز مطمئنا با گنجاندن آن در فهرست مشکل داشتم. اما متأسفانه، عوامل انتشار اطلاعات نادرست عمدا به محتوای خود برچسب طنز می‌زنند تا اطمینان حاصل کنند که «راستی‌آزمایی» نخواهد شد و درعین‌حال از زیر بار مسئولیت هرگونه آسیب ناشی از این محتوا نیز شانه خالی می‌کنند.

در یک اکوسیستم اطلاعاتی که در آن بستر بحث و نشانه‌ها، یا میانبرهای ذهنی (فرآیندهای کاوش و اکتشافات) به‌کلی حذف شده‌اند، احتمال اینکه محتوای طنز خواننده را گیج کند بیشتر است. یک فرد آمریکایی ممکن است بداند که وب‌سایت Onion یک سایت طنز است، اما آیا می‌دانستید که ۵۷ وب‌سایت خبری طنز در سراسر دنیا وجود دارد؟ اگر اطلاع نداشته باشید محتوای یک وب‌سایت طنز است و در فید فیس‌بوک خود به آن برخورد کنید، فریب خوردن ساده است.

اخیرا فیس‌بوک تصمیم گرفته است محتوای طنز را راستی‌آزمایی نکند، اما کسانی که در این فضا فعالیت می‌کنند به‌خوبی می‌دانند چگونه از زدن برچسب طنز به‌عنوان یک ترفند استفاده می‌شود. درواقع در آگوست سال ۲۰۱۹ نهاد فکت‌چکینگ اسنوپس در ایالات متحده مقاله‌ای در این مورد منتشر کرد که توضیح می‌داد چرا محتوای طنز را راستی‌آزمایی می‌کند. محتوایی که ادعا می‌شود طنز است از درستی‌سنجی شدن می‌گریزد، و اغلب با گذشت زمان زمینه و بستر اصلی آن فراموش می‌شود: مردم محتوا را به اشتراک می‌گذارند و باز هم به اشتراک می‌گذارند بدون اینکه متوجه باشند طنز است و باور می‌کنند که واقعیت دارد.

ارتباط ساختگی

این یک تله کلیک قدیمی است: به این صورت که در تیتری هیجان‌انگیز ادعایی در مورد محتوا مطرح می‌شود، اما در واقع تیتر هیچ ارتباطی با محتوا یا مقاله ندارد. البته که رسانه‌های خبری می‌توانند به‌راحتی مشکل اختلال اطلاعاتی را به عاملان بد و نامطلوب نسبت دهند، اما به‌عقیده‌ی من مهم است بدانیم که شیوه‌های ضعیف روزنامه‌نگاری نیز می‌توانند به چالش‌های آشفتگی اطلاعات دامن بزنند.

محتوای گمراه‌کننده

این چیزی است که همیشه در روزنامه‌نگاری و سیاست مشکل‌ساز بوده است. از انتخاب یک بخش جزئی از یک نقل‌قول گرفته تا ایجاد آماری که ادعای خاصی را پشتیبانی می‌کند اما نحوه به وجود آمدن مجموعه‌داده را در نظر نمی‌گیرد، یا برش عکس برای نشان دادن یک رویداد به شکلی خاص، این روش‌های گمراه‌کننده هیچکدام نو و بی‌سابقه نیستند.

بستر و زمینه‌ی نادرست

بخش عمده‌ی محتواهای نادرست از این نوع هستند. این اختلال در اطلاعات اغلب زمانی رخ می‌دهد که یک تصویر واقعی اما قدیمی به‌عنوان تصویری جدید ارائه می‌شود. به‌اشتراک گذاشتن تصاویر قدیمی به جای تصاویر جدید اغلب در ارتباط با رویدادهای خبری فوری اتفاق می‌افتد، اما گاهی نیز مقاله‌های قدیمی که تیتر آن‌ها همچنان مرتبط با وقایع روز به نظر می‌رسد به‌عنوان مقاله‌ی جدید بازنشر می‌شوند.

محتوای تقلبی

این اختلال زمانی روی می‌دهد که از لوگوی یک برند یا یک نام شناخته‌شده در کنار محتوای نادرست استفاده می‌شود. دلیل استراتژیک بودن این تاکتیک اتکای آن بر فرآیندهای کاوشی و اکتشافی ذهن است. یکی از بهترین روش‌های قضاوت درباره‌ی محتوا این است که ببینیم آیا توسط سازمان یا فردی ارائه شده که از پیش به آن‌ها اعتماد داشتیم. بنابراین، با گرفتن لوگوی یک سازمان خبری مورد اعتماد و افزودن آن به یک عکس یا یک ویدیو، به‌طور خودکار شانس اعتماد افراد به آن بدون بررسی‌های بیشتر افزایش پیدا می‌کند.

محتوای دستکاری‌شده

این زمانی است که محتوای واقعی به نوعی دستکاری یا ادیت می‌شود. ویدئوی نانسی پلوسی مربوط به ماه مه ۲۰۱۹ نمونه‌ای از این موارد است. این فیلم رییس مجلس نمایندگان آمریکا را در حال سخنرانی نشان می‌دهد. تنها چند ساعت بعد از ویدئوی اول، ویدئوی دیگری منتشر شد که نشان می‌داد ظاهرا او در هنگام سخنرانی مست بوده است. درواقع، سرعت این ویدئو کاهش داده شده بود و همین باعث می‌شد اینطور به نظر برسد که او در بیان کلمات مشکل دارد. این ترفند به دلیل استفاده از یک ویدئوی واقعی قدرتمند است. اگر مردم از سخنرانی پلوسی اطلاع داشته باشند، باور نتیجه و حاصل دستکاری محتوا برایشان ساده‌تر می‌شود.

محتوای ساختگی

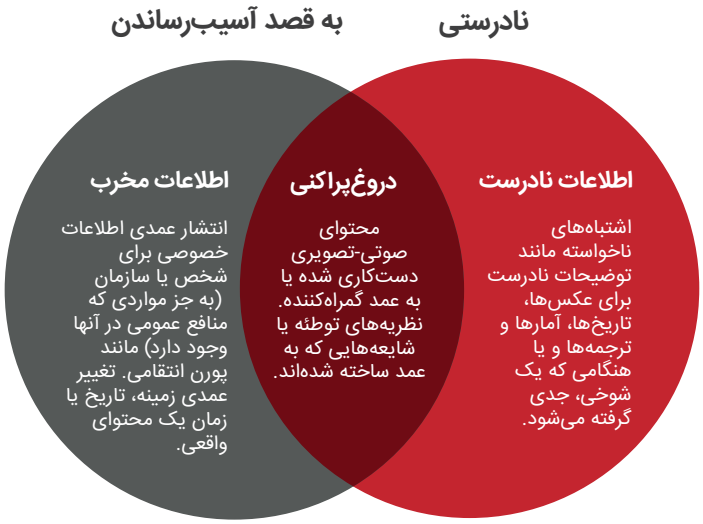
این دسته از اختلال اطلاعات به مواردی اشاره دارد که محتوا صد در صد ساختگی است. این کار ممکن است از طریق ایجاد یک حساب کاربری جعلی کاملا جدید در شبکه‌های اجتماعی و انتشار محتوای جدید از طریق آن صورت بگیرد. این دسته همچنین شامل دیپ‌فیک‌ها (جعل عمیق) نیز می‌شود: ویدئوها یا صوت‌هایی که با استفاده از هوش مصنوعی تولید می‌شوند و شخصی را در حال گفتن حرف یا انجام کاری نشان می‌دهند که هرگز صورت نگرفته است.

درک قصد و انگیزه

انواع اختلال اطلاعات که در بالا ذکر شد برای توضیح پیچیدگی محیط اطلاعاتی آلوده مفید هستند، اما به توضیح قصد و انگیزه‌ی عاملان کمکی نمی‌کنند؛ مسئله‌ای که بخش مهمی از درک این پدیده است. برای انجام این کار، من و درخشان نمودار زیر را به‌عنوان راهی برای توضیح تفاوت بین اطلاعات نادرست، دروغ‌پراکنی و اصطلاح سومی که ایجاد کرده‌ایم، یعنی اطلاعات بد، طراحی کرده‌ایم. اطلاعات نادرست (میس‌اینفورمیشن) و دروغ‌پراکنی (دیس‌اینفورمیشن) هر دو نمونه‌هایی از محتوای تقلبی هستند. اما دروغ‌پراکنی توسط افرادی صورت می‌گیرد که قصد آسیب رساندن دارند، خواه این آسیب مالی باشد، خواه آسیب به آبروی افراد یا آسیب سیاسی و یا جسمی. اطلاعات نادرست نیز تقلبی هستند اما کسانی که آن را پراکنده می‌کنند از نادرست بودن آن اطلاع ندارند. این اتفاق اغلب در زمان وقوع رویدادهای خبری فوری روی می‌دهد، زمانی که افراد عکس‌ها و شایعات قدیمی را بی‌آنکه بدانند به‌عنوان محتوای مرتبط با رویدادهای اخیر به اشتراک می‌گذارند.

اطلاعات مخرب، اطلاعات واقعی هستند اما هدف از به اشتراک گذاشتن آن‌ها آسیب رساندن است. فاش شدن ایمیل‌های هیلاری کلینتون در جریان انتخابات ریاست‌جمهوری سال ۲۰۱۶ آمریکا نمونه‌ای از آن است. انتشار انتقام‌جویانه‌ی ویدئوی روابط جنسی نیز می‌تواند نمونه‌ی دیگری باشد.

گونه‌های متداول آشفتگی اطلاعات



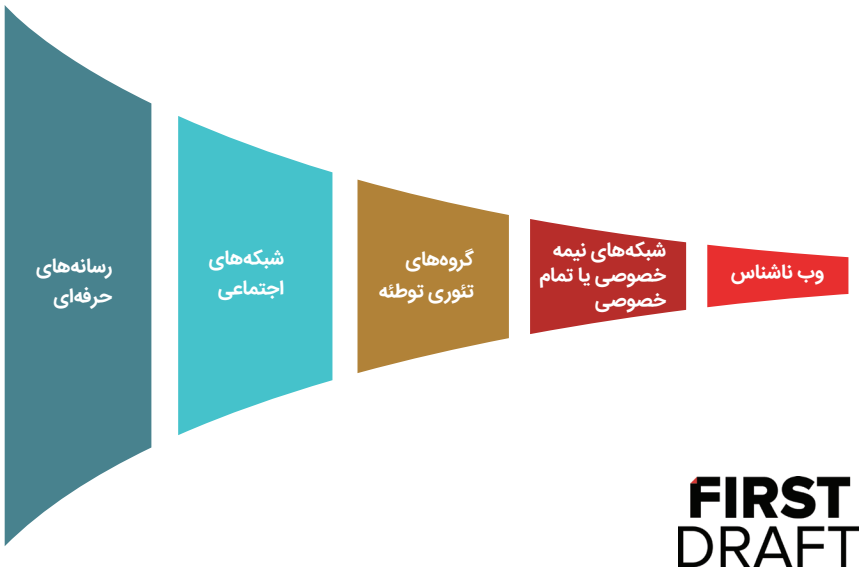
این اصطلاحات مهم هستند، زیرا قصد منتشرکننده بخشی از درک ما در خصوص یک قطعه‌ی خاص از اطلاعات را

شکل می‌دهد. سه انگیزه‌ی اصلی برای ایجاد محتوای نادرست و گمراه کننده وجود دارد. اولی انگیزه‌ی سیاسی است، چه سیاست خارجی و چه داخلی. به‌عنوان مثال، تلاش یک دولت خارجی برای مداخله در انتخابات کشوری دیگر. قصد و انگیزه ممکن است داخلی باشد، مثلا استفاده‌ی یک کمپین از تاکتیک‌های «کثیف» برای لکه‌دار کردن حریف. دومین انگیزه، انگیزه‌ی مالی است. افراد می‌توانند از طریق تبلیغات بر روی وب‌سایت خود درآمد کسب کنند. اگر مقاله‌ی نادرستی با یک عنوان بسیار جذاب داشته باشید، تا زمانی که بتوانید مردم را وادار کنید روی لینک شما کلیک کنند، می‌توانید درآمد کسب کنید. افرادی از هر دو سر طیف سیاسی اعتراف کرده‌اند که چگونه سایت‌های «خبری» ساختگی را برای افزایش کلیک و در نتیجه درآمد ایجاد کرده‌اند. درنهایت، انگیزه‌ها و عامل روانی و اجتماعی نیز در این میان نقش دارند. برخی افراد صرفا دوست دارند دردسر ایجاد کنند و ببینند تا کجا می‌توانند قسر در بروند؛ آن‌ها می‌خواهند ببینند آیا می‌توانند روزنامه‌نگاران را فریب بدهند، یا رویدادی در فیس‌بوک ایجاد کنند که مردم را برای اعتراض به خیابان‌ها بکشاند و یا زنان را آزار و اذیت کنند؟ برخی دیگر به این دلیل اطلاعات نادرست را به اشتراک می‌گذارند که مایلند هویت خاصی برای خودشان بسازند. به‌عنوان مثال کسی که می‌گوید: «برام مهم نیست این درست است یا نیست، فقط می‌خوام به دوستانم در فیس‌بوک تأکید بکنم که چه‌قدر حالم از فلان نامزد انتخاباتی به هم می‌خوره».

شیپور تقویت

برای داشتن درکی درست از این اکوسیستم گسترده، لازم است به ماهیت درهم‌تنیده‌ی آن توجه کنیم. اغلب اوقات فرد محتوای گمراه‌کننده و نادرست را در جایی می‌بیند و گمان می‌کند که در همانجا تولید شده است. متأسفانه، کسانی که می‌دانند چگونه به شکل مؤثری از تکنیک‌های دروغ‌پراکنی استفاده کنند، روش‌های سود بردن از ماهیت گسیخته و تکه‌تکه‌ی این اکوسیستم را به‌خوبی بلدند.

این را نیز به خاطر داشته باشید که اطلاعات نادرست، تئوری‌های توطئه و شایعات اگر پراکنده نمی‌شدند آسیبی نداشتند. به اشتراک گذاشتن آن‌ها است که بیشترین آسیب را ایجاد می‌کند. به همین دلیل من شکل زیر را، که اسمش را شیپور تقویت (Amplifying Trumpet) گذاشته‌ام، برای نشان دادن نحوه‌ی استفاده‌ی عاملان بد از هماهنگی برای انتقال اطلاعات در اکوسیستم طراحی کرده‌ام.



اغلب، محتوا در فضاهایی مانند فورچَن (4chan) یا دیسکورد (برنامه‌ای که توسط گیمرها برای ارتباط با یکدیگر استفاده می‌شود) پست می‌شود. افراد در این فضاها ناشناس هستند و می‌توانند بدون ذکر منبع مطلب خود را پست کنند. اغلب از این فضاها برای به اشتراک گذاشتن جزئیات خاص جهت هماهنگی استفاده می‌شود، مثلا «سعی خواهیم کرد این هشتگ خاص را ترند کنیم» یا «از این میم برای پاسخ به رویدادهای امروز در فیس‌بوک استفاده می‌کنیم».

سپس در مراحل بعدی، هماهنگی از طریق پیام‌های خصوصی مستقیم در توییتر یا واتس‌اپ به چندین کاربر به‌صورت هم‌زمان در پی گرفته می‌شود، جایی که گروه‌های درون یک شبکه، محتوا را به گروه وسیع‌تری از افراد پخش می‌کنند. از آنجا محتوا به گروه‌هایی در شبکه‌هایی مانند گب، ردیت و یا یوتیوب منتقل و بعد در شبکه‌های اصلی‌تر از جمله فیس‌بوک، اینستاگرم یا توییتر پخش می‌شود.

معمولا در این مرحله توجه رسانه‌های حرفه‌ای به دو دلیل به محتوا جلب می‌شود؛ یا به این دلیل که منبع محتوا را نمی‌شناسند و بدون بررسی‌های کافی تصمیم می‌گیرند از آن در گزارش‌های خود استفاده کنند، و یا به این دلیل که تصمیم می‌گیرند محتوا را بی‌اعتبار کنند. در هر دو صورت عوامل انتشار محتوای نادرست این جلب توجه را یک موفقیت به حساب می‌آورند. تیترهای ضعیفی که شایعه یا ادعای گمراه‌کننده را تکرار و گزارش می‌کنند و یا نشان می‌دهند که اطلاعات نادرست در کجای داستان

پنهان شده است، در واقع به طرح و نقشه‌ی اصلی کمک می‌کنند: تقویت محتوا و هیزم ریختن به آتش شایعه.

در First Draft ما از مفهوم نقطه‌ی عطف یا نقطه‌ی بحران استفاده می‌کنیم. اگر روزنامه‌نگاران زودتر از موعد مناسب به اطلاعات نادرست واکنش نشان بدهند آتش شایعات را تندتر می‌کنند و این قطعا آسیب‌رسان خواهد بود. از طرف دیگر، اگر بیش از اندازه برای واکنش نشان دادن درنگ کنند، ادعای نادرست و شایعات پا می‌گیرند و دیگر کار چندانی از دستشان ساخته نخواهد بود. بنابراین تشخیص این نقطه‌ی بحران بسیار دشوار است و بسته به مکان، موضوع و پلتفرم می‌تواند متفاوت باشد.

نتیجه‌گیری

زبان، پدیده‌ای مهم و پیچیده است. واژگانی که استفاده می‌کنیم می‌توانند در نتیجه‌ی حاصله تفاوت ایجاد کنند. مطالعات دانشگاهی اخیر نشان می‌دهد مخاطبان بیشتر از گذشته اصطلاح اخبار جعلی را با شیوه‌های ضعیف گزارشگری در رسانه‌های حرفه‌ای برابر می‌دانند.

توصیف هر محتوایی به‌عنوان اطلاعات دروغ، درحالیکه ممکن است آن اطلاعات کاملا نادرست نباشد و یا توسط کاربرانی به اشتراک گذاشته شود که از نادرست بودن آن آگاه نیستند، از دیگر عناصر مهم در درک رویدادهای درحال وقوع در فضای دیجیتال هستند.

ما در عصر آشفتگی اطلاعات زندگی می‌کنیم؛ عصری که چالش‌های جدیدی را پیش روی روزنامه‌نگاران، محققان و متخصصان اطلاعات قرار داده است. گزارش کردن یا گزارش نکردن؟ چگونه تیترها را انتخاب کنیم؟ چگونه فیلم‌ها و تصاویر نادرست را به‌طور مؤثر بی‌اعتبار کنیم؟ چگونه بفهمیم چه زمانی باید بی‌اعتبارسازی صورت بگیرد؟ چگونه نقطه‌ی بحران را تشخیص دهیم؟ همه‌ی این‌ها چالش‌های جدیدی هستند که امروزه بر سر راه کسانی که در محیط اخبار و اطلاعات کار می‌کنند وجود دارد. مسئله پیچیده‌ای است.

چرخه‌ی حیات دستکاری‌های رسانه‌ای

نوشته‌ی: **جوآن دانوان**

دکتر جوآن دانوان مدیر تحقیقات مرکز شورنستاین در دانشکده‌ی کندی هاروارد برای رسانه، سیاست و سیاست‌گذاری‌های عمومی است.

در عصری که تعداد انگشت‌شماری پلتفرم قدرتمندِ فناوریِ جهانی ابزارهای سنتی اطلاع‌رسانی جامعه را مختل کرده‌اند، کارزارهای دستکاری رسانه‌ای و اطلاعات نادرست مشکلاتی بر سر راه همه‌ی نهادهای سیاسی و اجتماعی ایجاد کرده است.

گروهی متشکل از فعالان سیاسی، برندها، جنبش‌های اجتماعی و «ترول»های غیروابسته که تکنیک‌های جدیدی برای اثرگذاری بر گفتمان‌های فضای عمومی ایجاد کرده‌اند، با استفاده از حقه‌ها و محتواهای ساختگی در مقیاس محلی، ملی و جهانی خرابی به بار می‌آورند. درخصوص اینکه دستکاری رسانه‌ای و اطلاعات نادرست مشکلات مهمی هستند که جامعه‌ی امروز با آن‌ها دست وپنجه نرم می‌کند توافق گسترده‌ای وجود دارد. اما تعریف، شناسایی، مستندسازی و بی‌اعتبار کردن اخبار نادرست و دستکاری‌های رسانه‌ای کار دشواری است، خصوصا که این فعالیت‌ها اغلب حوزه‌های متنوعی، از روزنامه‌نگاری گرفته تا حقوق و فناوری، را هدف قرار می‌دهند. بنابراین، درک دستکاری‌های رسانه‌ای به‌عنوان فعالیت‌هایی با الگوی خاص اولین گام اساسی برای بررسی، افشاء و کاهش اثرات آن‌هاست.

تعریف دستکاری رسانه‌ای و اطلاعات نادرست

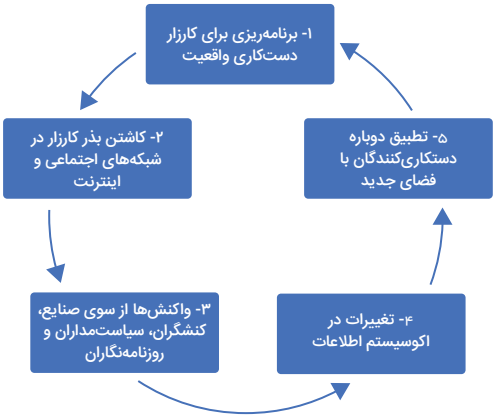
برای ارائه‌ی تعریفی از اصطلاح دستکاری رسانه‌ای ابتدا باید این اصطلاح را به دو بخش مجزا تقسیم کنیم. رسانه در عام‌ترین معنای خود نوعی ابزار ارتباطی است. متون، تصاویر، صداها و ویدئوهای در قالب فیزیکی و دیجیتال نمونه‌هایی از آن هستند. هنگام مطالعه‌ی رسانه، هر اثر و رد به‌جامانده‌ای می‌تواند به‌عنوان مدرک ثبت‌شده‌ی یک رویداد استفاده شود. اساسا رسانه‌ها توسط افراد به منظور

برقراری ارتباط ایجاد می‌شوند. بنابراین، رسانه وسیله‌ی انتقال معنا به افراد است، اما تفسیر معنا همیشه نسبی است و در زمینه و بستر خاص انتشار آن صورت می‌گیرد.

ادعای دستکاری شدن رسانه به چیزی فراتر از این واقعیت اشاره می‌کند که رسانه‌ها توسط افراد برای انتقال معنای خاصی ایجاد شده‌اند. فرهنگ لغات مریام-وبستر واژه‌ی دستکاری را اینطور تعریف می‌کند: «تغییر به شکلی هنرمندانه و یا از طرق غیرمنصفانه برای نیل به هدف خاص». اگرچه گاهی اوقات پی بردن به هدف خاصی که یک محصول مشخص برای رسیدن به آن ساخته شده می‌تواند دشوار باشد، محققان می‌توانند مشخص کنند چه کسی چه چیزی را کجا و چگونه منتقل کرده است و از این راه مشخص کنند آیا ترفندهای دستکاری به‌عنوان بخشی از فرآیند توزیع آن استفاده شده‌اند یا خیر. ترفندهای دستکاری می‌تواند شامل پنهان کردن هویت ناشر یا منبع محتوا، ویرایش برای پنهان کردن یا تغییر معنا یا زمینه‌ی واقعی یک محتوا و دستکاری الگوریتم‌ها با استفاده از هماهنگی مصنوعی (به‌عنوان مثال، از طریق ربات‌ها و ابزارهای ارسال هرزنامه) باشد.

در این بستر، اطلاعات نادرست یکی از زیرشاخه‌های دستکاری رسانه‌ای است و به ایجاد و توزیع عمدی اطلاعات غلط برای نیل به اهداف سیاسی اشاره دارد. فناوران، کارشناسان، پژوهش‌گران، روزنامه‌نگاران و سیاست‌گذاران باید در مورد دسته‌ی خاصی از اطلاعات به نام اطلاعات نادرست به توافق برسند، زیرا تلاش برای مبارزه با اطلاعات نادرست مستلزم همکاری این گروه‌ها است.

تیم تحقیقات فناوری و تغییر اجتماعی (TaSC) در مرکز شورنستاینِ دانشکده‌ی کندی هاروارد به نوبه‌ی خود، از رویکرد مطالعه‌ی موردی برای ترسیم چرخه‌ی حیات کارزارهای دستکاری رسانه‌ای استفاده می‌کند. هدف این رویکردِ روش‌شناختی، تحلیل ترتیب، مقیاس و دامنه کمپین‌های دستکاری از طریق دنبال کردن محصولات رسانه‌ای در طول زمان و مکان است و برای نظم دادن به این آشفتگی درهم‌تنیده، روابط متعددی را کنار هم می‌چینند. به‌عنوان بخشی از کار، شِمایی کلی از چرخه‌ی حیات یک کارزار دستکاری رسانه‌ای ایجاد کرده‌ایم که برای روزنامه‌نگارانی که تلاش می‌کنند دستکاری‌های رسانه‌ای و اطلاعات نادرست را شناسایی، ردیابی و افشاء کنند مفید خواهد بود.



چرخه‌ی حیات یک کمپین دستکاری رسانه‌ای

این چرخه‌ی حیات دارای پنج نقطه‌ی عملیاتی است که می‌توان ترفندهای دستکاری رسانه‌ای را با استفاده از روش‌های کمی و کیفی در آن‌ها مستند کرد. توجه داشته باشید که اکثر کمپین‌های دستکاری با همین ترتیب «کشف» نمی‌شوند. در هنگام تحقیق، باید به دنبال هر یک از این نقاط عمل باشید و سپس کمپین را در طول چرخه‌ی زندگی آن به عقب و جلو دنبال کنید.

مطالعه‌ی موردی: افشاگری

بیایید فعالیت‌ها در رسانه‌های اجتماعی را پیرامون شکایت فرد افشاگری که درباره‌ی فعالیت‌های رئیس‌جمهور دونالد ترامپ در رابطه با اوکراین افشاگری کرده بود بررسی کنیم تا ببینیم چگونه یک کارزار دستکاری رسانه‌ای افشاء می‌شود و چگونه اقدامات اخلاقی روزنامه‌نگاران و پلتفرم‌ها در اوایل چرخه‌ی زندگی دستکاری رسانه‌ای می‌تواند به خنثی کردن تلاش‌ها برای دستکاری کمک کند.

برنامه‌ریزی و بذرپاشی (مراحل ۱ و ۲): در اکوسیستم رسانه‌ای تئوری توطئه، هویت افشاگر از قبل مشخص است و نام او در وبلاگ‌ها، توئیتر، فیس‌بوک، ویدئوهای یوتیوب و اتاق‌های گفتگو پخش می‌شود. نکته‌ی مهم این است که نام‌های خاص می‌توانند جایگزین کلیدواژه‌ها و هشتگ‌ها شوند و به‌عنوان نقاط‌داده‌ی قابل‌جستجوی غیروابسته عمل کنند. بنابراین، تلاشی هماهنگ از پیش برای انتشار نام مورد نظر و عکس شخص صورت می‌گیرد. بااین‌حال، در این مورد خاص به نظر می‌رسد این نام در اتاق پژواک حساب‌های کاربری مرتبط با نهادهای جناح راست و نهادها و حساب‌های کاربری توطئه‌ای در رسانه‌ی آنلاین گیر کرده است و با وجود تلاش هماهنگ‌شده‌ی اینفلوئنسرهای توطئه برای وارد کردن نام افشاگر ادعایی به جریان اصلی، آن‌ها موفق نشدند محتوا را از حباب فیلترهای خود خارج کنند. چرا این اتفاق رخ می‌دهد؟

پاسخ خبرنگاران، فعالان و غیره (مرحله ۳): در مقابل، رسانه‌های چپ و میانه‌رو از انتشار نام افشاگر ادعایی پرهیز کردند و ادعاهای مبنی بر برملا شدن هویت او را تقویت نکردند. اگرچه این یک داستان خبرساز برای خبرنگاران فعال در زمینه‌ی فناوری و سیاست بود، بااین‌حال رسانه‌های اصلی از جلب توجه به نام این شخص در اکوسیستم رسانه‌های اجتماعی خودداری کردند. در مواردی که این مطلب پوشش داده شد نیز اکثرا تأکید بر این بود که پخش و پراکنده کردن این نام درواقع برای دستکاری بحث پیرامون شکایت این افشاگر بوده است و از انتشار نام فرد اجتناب می‌شد. این امر تا حد زیادی به اخلاق روزنامه‌نگاری مربوط می‌شود، جایی که خبرنگاران وظیفه ویژه‌ای برای محافظت از ناشناس بودن منابع دارند و این اصل اخلاقی به افشاگران نیز تسری پیدا می‌کند.

تغییرات در اکوسیستم اطلاعات (مرحله‌ی ۴): اگرچه روزنامه‌نگاران جریان اصلی نام را حذف می‌کردند، نام ادعایی افشاگر، «اریک سیاراملا» یک کلمه‌ی کلیدی خاص و منحصربه‌فرد است. این بدان معناست که افرادی که آن را جستجو می‌کنند می‌توانند به مطالب متنوعی که ریشه در دیدگاه متأثر از توطئه دارد، دست پیدا کنند. بنابراین، علاوه بر روزنامه‌نگاران اخلاق‌مداری که فعالانه از پرداختن به داستان، که می‌توانست ترافیک رسانه‌ای قابل‌تجهی را جلب کند، خودداری کردند پلتفرم‌های مختلف اینترنتی نیز محتوایی را که از نام افشاگر ادعایی به عنوان کلمه‌ی کلیدی استفاده می‌کرد، فعالانه تعدیل کردند.

یوتیوب و فیس‌بوک محتوایی را که از نام او استفاده می‌کرد حذف کردند و توئیتر از ترند شدن نام او جلوگیری کرد. جستجوی گوگل امکان جستجوی نام او را مسدود کرد و هزاران لینک را به وبلاگ‌های توطئه بازگرداند.

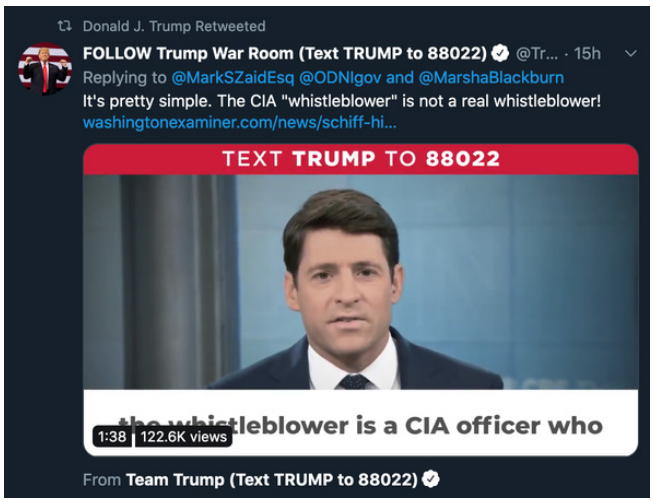
تنظیمات جدید دستکاری‌کنندگان (مرحله‌ی ۵): این اقدامات برای جلوگیری از انتشار اطلاعات نادرست دستکاری‌کننده‌ها را بیشتر تهییج کرد و باعث شد ترفندهای خود را تغییر بدهند.

به‌جای پافشاری بر انتشار نام افشاگر ادعایی، دستکاری‌کنندگان شروع به پخش عکس‌هایی از یک مرد سفید پوست متفاوت (با عینک و ریش) کردند که شبیه عکسی بود که قبلاً با نام افشارگر ادعایی منتشر شده بود. این عکس‌های جدید با روایتی توطئه‌آمیز همراه بود که حکایت از وجود یک ,دولت پنهان, (دولتِ قدرتمندتر از دولتِ انتخابی) داشت و ادعا می‌کرد افشاگر رفیق شفیق دموکرات‌های حکومتی است و بنابراین انگیزه‌های حزبی دارد. اما درواقع، شخصی که در عکس‌ها دیده می‌شد الکساندر سوروس، پسر سرمایه‌گذار میلیاردر و خیّر جورج سوروس بود که بارها هدف توطئه‌های مکرر قرار گرفته بود.

هنگامی که این ترفند موفق نشد توجه رسانه‌ها را جلب کند، حساب توییتر رئیس‌جمهور ترامپ،

@RealDonaldTrump، مقاله‌ای را با نام افشاگر مظنون بازنشر کرد که به ۶۸میلیون دنبال‌کننده‌اش تاکید می‌کرد «افشاگر سیا (سی‌آی‌ای) یک افشاگر واقعی نیست!». توئیت اصلی از حساب کاربری @TrumpWarRoom منتشر شده بود که حساب رسمی و تأییدشده‌ی کمپین ترامپ است. این توئیت سیلی از پوشش رسانه‌ای را به دنبال داشت و از جمله بسیاری از رسانه‌های جریان اصلی تمام تلاش خود را برای حذف یا پوشش دادن افشاگر ادعایی به خرج دادند. بسیاری از مردم در رسانه‌های اجتماعی از افشاگر خواستند تا در جلسات استیضاح سنا شهادت دهد و بنابراین نامش در کنار نام سایر شاهدان بالقوه مهم مورد استناد قرار می‌گرفت و همین باعث می‌شد احتمال اینکه دیگران هنگام جستجوی نام‌های دیگر به آن برخورد کنند نیز بیشتر شود. و بدین ترتیب، چرخه‌ی جدیدی از دستکاری رسانه‌ای آغاز شد.

در این مرحله از چرخه‌ی حیات، جستجوی نام افشاگر ادعایی افزایش پیدا کرد و در وبلاگ‌ها تئوری‌توطئه‌های فراوانی در خصوص انگیزه‌های شخصی و حرفه‌ای او برای برملا کردن فعالیت‌های ترامپ به چشم می‌خورد. رویکرد خبرنگارانی که در مورد این توئیت‌ها گزارش می‌کنند بین بحث بر سر ارعاب شاهدان بحثی که ادعا می‌کند چنین اقداماتی می‌تواند باعث منصرف شدن افشارگران در آینده شود- از یک سو، و نوک زدن به کنجکاوی‌های هیجان‌انگیز در مورد شایعاتی که می‌گویند انگیزه‌ی ترامپ از رو کردن دست این افشاگر ادعایی چه بوده از سوی دیگر، در نوسان است. به‌این‌ترتیب، می‌توان گفت تلاش برخی رسانه‌ها برای پاسخگو کردن نخبگان قابل‌تقدیر است، اما انجام این کار نیز ممکن نیست مگر به قیمت پرداختن به این موضوع که چگونه محصولات رسانه‌ای خود آن‌ها تبدیل به ابزار سیاسی سودمندی برای دستکاری رسانه‌ای و انتشار اطلاعات نادرست شده است.



مستندسازی چرخه‌ی حیات

دستکاری‌کنندگان تلاش کردند با بارگذاری عکس‌ها و نام افشارگر در رسانه‌های اجتماعی کم‌کم امکان صعود و نشر آن در رسانه‌های مهم و جریان اصلی را فراهم کنند تا جایی که درنهایت رسانه‌های بزرگ و دارای وجاهت قانونی این محتوا را تقویت کنند و مطلب به ترند پلتفرم‌های مختلف تبدیل شده و به‌راحتی قابل کشف و دسترسی باشد. اما تصمیم‌ها و اقدامات روزنامه‌نگاران و پلتفرم‌ها باعث شد تلاش‌ها برای نشاندن نام و هویت افشاگر ادعایی در آگاهی جمعی و جریان اصلی به ثمر ننشیند تا اینکه یک شخصیت مهم و شناخته‌شده مطلب را بازنشر کرد. با آنکه بسیاری از سازمان‌های رسانه‌ای تلاش می‌کنند از دستورالعمل‌های اخلاقی پیروی کنند، رسانه‌های اجتماعی به سلاح قدرتمندان برای تنظیم انگیزه‌های رسانه‌ای و هدایت توطئه‌های خطرناک تبدیل شده‌اند.

اما روی‌هم‌رفته، این مطالعه‌ی موردی نشان‌دهنده‌ی پیشرفتی است که در مقایسه با موارد قبلی از این دست صورت گرفته است؛ زمانی که خبرنگاران در تلاش برای بی‌اعتبارسازی کارزارهای اطلاعات نادرست ناخواسته آن‌ها را تقویت می‌کردند و پلتفرم‌ها نیز هیچ وظیفه‌ای برای ارائه‌ی اطلاعات دقیق به مخاطبان احساس نمی‌کردند. این تغییر کلی امیدوارکننده است، اما جای پاسخگویی نخبگان هنوز در این میان خالی است. کشف، مستندسازی و افشای کمپین‌های دستکاری رسانه‌ها برای روزنامه‌نگاران و محققان به یک اندازه خطرناک است.. در این برهه از زمان که تقسیم‌بندی‌های حزبی به‌شدت پررنگ شده‌اند، هر ادعایی درخصوص یک کمپین اطلاعات نادرست می‌تواند هجوم ترول‌های فضای مجازی را به همراه داشته و باعث جلب توجه ناخواسته شود. دست و پنجه نرم کردن با محتوا و بستر اطلاعات نادرست مستلزم آن است که همگی‌مان اطلاعاتی را در خصوص چگونگی شروع، تحولات و پایان یک کمپین با دقت علمی و پشتکار مستند کنیم و این نکته را در نظر داشته باشیم که هر پایان مفروض برای یک کمپین، می‌تواند شروع ماجرای جدیدی باشد.

۱. بررسی حساب‌های کاربری در شبکه‌های اجتماعی

نوشته‌ی: **برندی زادرزنی**

برندی زادرزنی گزارشگر تحقیقی شبکه‌ی خبری اِن‌بی‌سی است و اغلب به پوشش کارزارهای دروغ‌پراکنی، اطلاعات نادرست و افراطی‌گرایی در اینترنت می‌پردازد.

تقریبا تمام داستان‌هایی که من گزارش می‌کنم به‌نوعی شامل کشف رد پای اشخاص در فضای مجازی است. از چک کردن پیشینه‌ی حساب‌های کاربری گرفته تا اخبار فوری و تحقیقات طولانی‌تر، شبکه‌های اجتماعی یکی از بهترین راه‌ها برای فهمیدن نکاتی درباره‌ی زندگی واقعی کاربران هستند؛ خانواده‌ی آن‌ها، دوستانشان، شغلشان، سیاست‌های شخصی و ارتباطاتشان. این شبکه‌ها همچنین پنجره‌هایی به دنیای افکار پنهانی و هویت‌های پنهان در فضای مجازی نیز هستند.

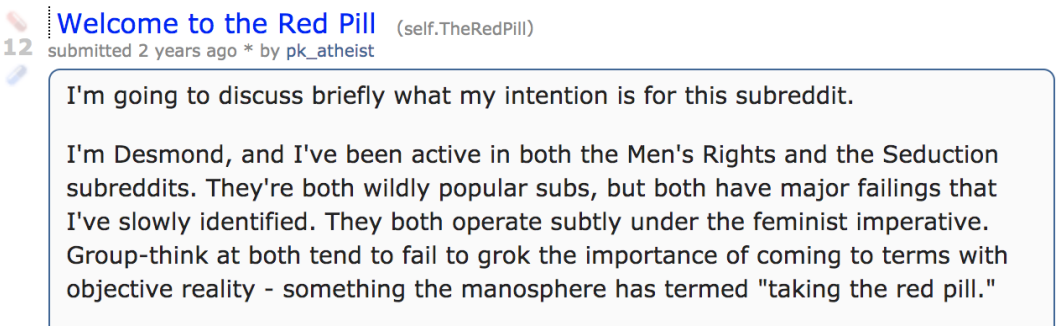
زمانه‌ی ما عصر فوق‌العاده‌ای برای روزنامه‌نگاران است. مردم هر روز بیش از پیش زندگی خود را در فضای مجازی می‌گذرانند و ابزارهای جستجو و کشف پروفایل‌های اجتماعی افراد همه‌جا هستند. درعین‌حال، هم مردم عادی و هم عاملان بد در پنهان کردن ردپای خود کارآزموده‌تر شده‌اند. در همین حین، در واکنش به اخبار منفی‌ای که در خصوص نقض حریم خصوصی کاربران و گسترش ایدئولوژی‌های زیان‌آور در شبکه‌های اجتماعی‌ای مانند فیس‌بوک منتشر شده است، این رسانه‌ها ابزارهایی را که روزنامه‌نگاران و محققان از آن‌ها برای کشف داستان‌ها و شناسایی افراد استفاده می‌کنند مسدود کرده‌اند.

در این فصل چند رویکرد اصلی برای بررسی حساب‌های کاربری در شبکه‌های اجتماعی را نشان خواهم داد. ابزارهایی که از آن‌ها نام می‌برم آن‌هایی هستند که در حال حاضر از آن‌ها استفاده می‌کنم اما احتمالا به‌زودی توسط فیس‌بوک مسدود می‌شوند و یا با ابزارهای بهتری جایگزین خواهند شد. گزارشگرانی که در این کار بهترین هستند، هرکدام فرایندها و ابزارهای خاص خود را برای رسیدن به نتیجه دارند، اما درواقع، مانند هر حیطه‌ی دیگری از گزارشگری، وسواس و کفش آهنی (البته به معنای استعاری) اغلب بهترین نتایج را به همراه دارد. اگر می‌خواهید سرنخ‌های کوچکی پیدا کنید

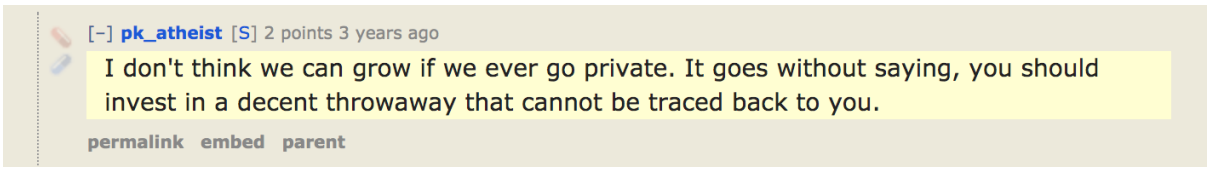
که در پاسخ به سؤال «این شخص کیست؟» کمکتان کند، آماده باشید برای خواندن هزاران توئیت، کلیک کردن روی نتایج جستجوی گوگل تا آخرین گزینه‌ی موجود و افتادن در باتلاق‌های گیج‌کننده‌ی رسانه‌های اجتماعی.

نام‌های کاربری

گاهی اوقات تنها سرنخی که در دست داریم یک نام کاربری است و البته ایرادی ندارد، چون درهرصورت همیشه باید از نام کاربری شروع کنیم. مورد فردی که زمانی نماینده‌ی جمهوری‌خواه نیوهمپشایر بوده و بنیان‌گذار یکی از محبوب‌ترین و بدنام‌ترین انجمن‌های مردان در سایت ردیت است، مثالی از همین وضعیت است. تحقیقات برای افشای هویت سازنده‌ی قرص قرمز، که حالا به انجمنی قرنطینه‌شده در ردیت تبدیل شده است، با استفاده از یک نام کاربری آغاز شد: pk-atheist



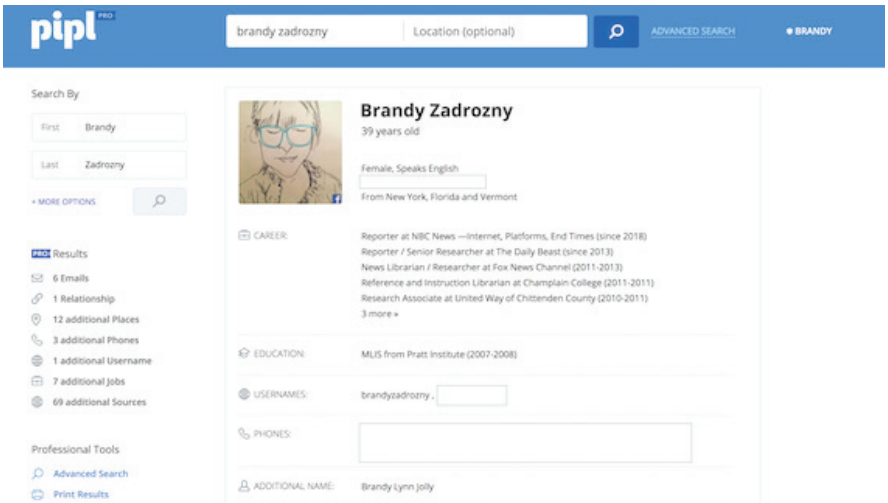
برخی افراد در پلتفرم‌ها و سیستم‌های ایمیل مختلف از یک نام کاربری تقریبا یکسان با تغییراتی جزئی استفاده می‌کنند. افرادی با تمرکز بیشتر بر روی مسائل امنیتی، مانند نماینده‌ی ایالت نیوهمپشایر، برای هر تلاش جدید خود نام‌های جدیدی را ایجاد و نام‌های قبلی را حذف می‌کنند.



در هر دو صورت، باید قبل از هر چیز نام کاربری مورد نظرتان را در چند وب‌سایت وارد کنید.

من ابتدا نام کاربری را در گوگل وارد کردم. افراد، خصوصا جوان‌ترهایی که از پلتفرم‌های اجتماعی بزرگ‌تر حذر می‌کنند، اغلب ردپایی از خود در غیرمنتظره‌ترین جاها به جا می‌گذارند، به‌عنوان مثال در بخش نظرات کاربران، اظهارنظرها و فروم‌ها. این سرنخ‌ها می‌توانند شما را به اطلاعات و حساب‌های کاربری مرتبط دیگر راهنمایی کنند.

در کنار جستجوی گوگل، از خدمات اختصاصی نیز استفاده کنید. این خدمات هزینه دارند و بسته به بودجه‌ی اتاق خبر شما، ممکن است به آن‌ها دسترسی داشته و یا نداشته باشید. Pipl و Skopenow از بهترین ابزارهایی هستند که برای مقابله‌ی اطلاعات «دنیای واقعی»، مانند شماره تلفن و سوابق دارایی، با سوابق آنلاین مانند ایمیل و نام کاربری پیدا کرده‌ام و هر دو در سطح جهانی کار می‌کنند. این موتورهای جستجوی پولی اغلب سوابق تلفن و دارایی‌ها را ارائه می‌دهند، اما می‌توانند بقایای حساب‌های کاربری فیس‌بوک و لینکدین را هم حتی پس از بسته شدن حساب کاربری شناسایی کنند. آن‌ها حتی حساب‌های کاربری‌ای که افراد فراموش کرده‌اند، مانند وبلاگ‌های قدیمی و لیست خرید آمازون، را نیز به هم متصل می‌کنند_یک معدن طلا برای فهمیدن اینکه فرد چه می‌خواند، چه چیزهایی می‌خرد و چه چیزهایی می‌خواهد. البته از طریق این ابزار موارد مثبت کاذب زیادی دریافت خواهید کرد؛ برای همین است که من تحقیقاتم را با نتایج آن‌ها شروع می‌کنم و بعد به سراغ تأیید گرفتن از طریق روش‌های دیگر می‌روم.

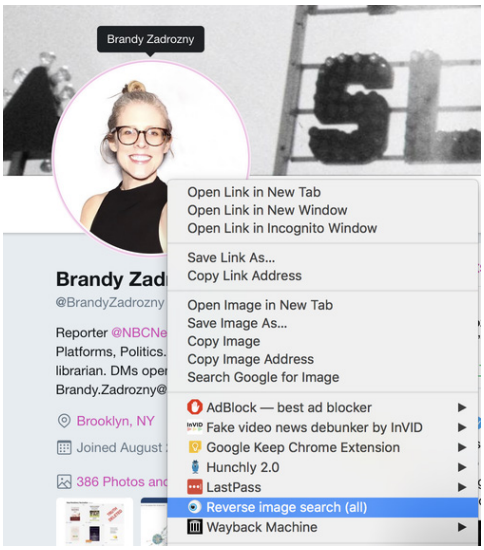


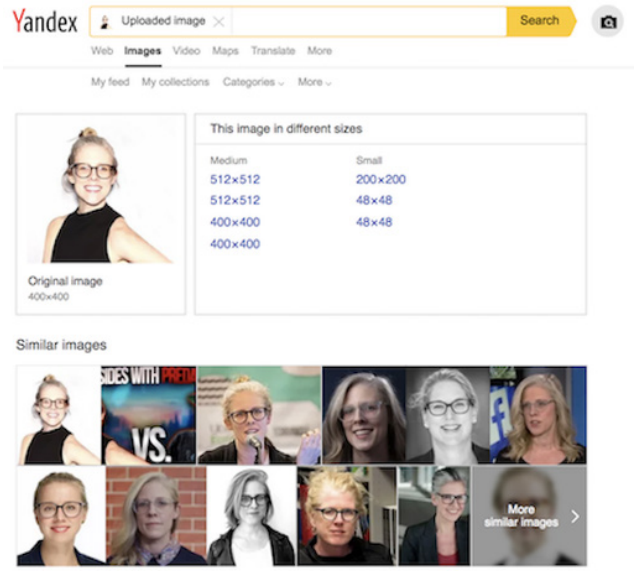
وقتی نام کاربری یا ایمیلی را پیدا می‌کنم که احتمال می‌دهم ممکن است به فرد مورد نظر من تعلق داشته باشد، آن را در یک ابزار آنلاین مانند namechk یا namecheckr وارد می‌کنم که وجود نام کاربری را در چندین پلتفرم مختلف بررسی می‌کنند. این ابزارها به گونه‌ای طراحی شده‌اند که بازاریابان با استفاده از آن‌ها بتوانند به راحتی بررسی کنند آیا نام کاربری مشخصی که قصد ثبتش را دارند در پلتفرم‌های مختلف موجود است یا خیر. اما این ابزارها برای بررسی اینکه آیا نام کاربری‌ای که در حال بررسی‌اش هستید در جای دیگری هم ثبت شده یا خیر نیز مفید هستند. بدیهی است که صِرف ثبت شدن یک نام کاربری در چندین پلتفرم به این معنی نیست که همه‌ی این حساب‌ها متعلق به یک شخص هستند. اما این یک نقطه شروع عالی برای جستجو در پلتفرم‌های مختلف است.

برای بررسی بیشتر نام کاربری، haveibeenpwned.com و Dehashed.com وجود دارند که اطلاعات کاربرانی را که حریم خصوصی‌شان نقض شده است ارائه می‌کنند و می‌توانند راهی سریع برای اعتبارسنجی آدرس ایمیل و ارائه سرنخ‌های جدید باشند.

عکس‌ها

نام کاربری همیشه به‌تنهایی برای ادامه‌ی تحقیقات کافی نیست. به‌علاوه، هیچ‌چیز نمی‌تواند به اندازه‌ی یک عکس تأثیرگذار و قانع‌کننده باشد. استفاده از عکس اشخاص راه دیگری برای تعیین هویت آن‌ها در پلتفرم‌های گوناگون است. جستجوی معکوس تصاویر در گوگل روش بدی نیست، اما موتورهای جستجوی دیگر-به‌ویژه موتور جستجوی روسی Yandex- ممکن است نتایج بهتری به دست دهند. من از افزونه‌ی Reveye Chrome استفاده می‌کنم که به من امکان می‌دهد روی یک تصویر کلیک راست کرده و مطابقت آن را در چندین پلتفرم از جمله Google، Bing، Yandex، و Tineye جستجو کنم. افزونه Search by Image همچنین دارای یک عملکرد ضبط دقیق است که به شما امکان می‌دهد یک تصویر را در تصویری دیگر جستجو کنید.



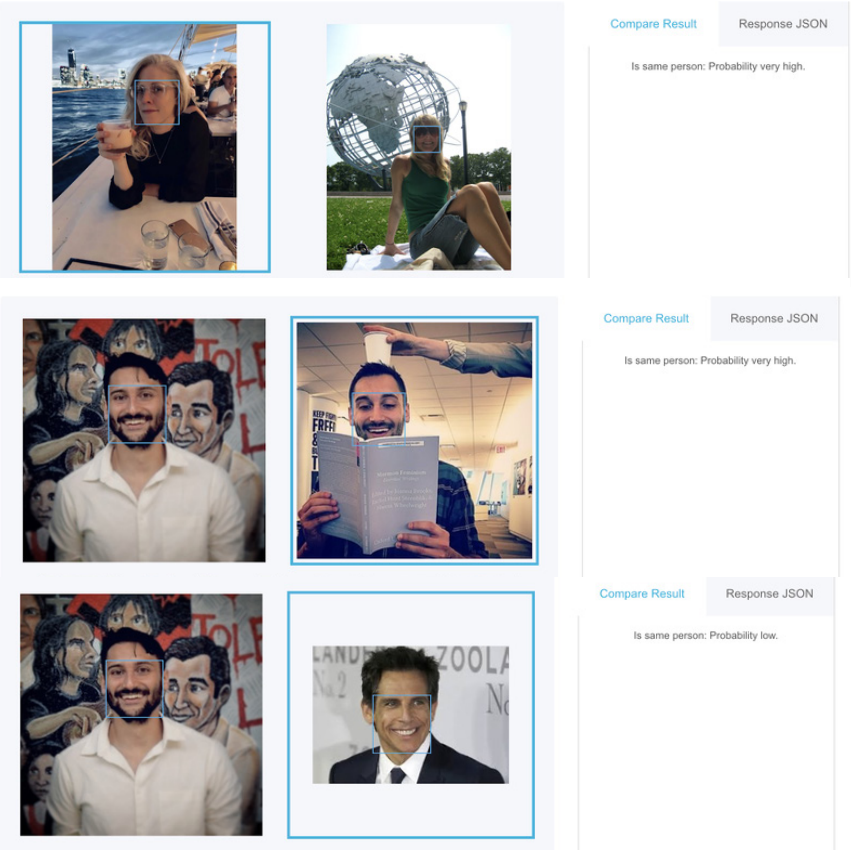


جستجوی معکوس تصاویر اشکالات خاص و عدیده‌ی خودش را دارد. موتورهای جستجویی که در بالا نام بردیم عملکرد ضعیفی در جستجوی تصاویر در توئیتر دارند و برای نمایش نتایج از سایت‌هایی مانند اینستاگرام و فیس‌بوک هم بی‌فایده هستند.

آنچه من اغلب به دنبالش هستم، جستجو و مقایسه‌ی تصاویر مختلف افراد است. نمی‌توانم بگویم تابه‌حال چند بار به صفحه‌ی نمایش کامپیوترم خیره شده‌ام، چشم‌ها را تنگ کرده و از همکارم

پرسیده‌ام: «به نظرت این شخص همون یکیه؟»

من نمی‌توانم فقط به چشم‌هایم اطمینان کنم. شناسایی ویژگی‌های ظاهری افراد از جمله خال‌ها یا ریش و سبیل می‌تواند مفید باشد. اخیرا، ترجیح می‌دهم از یک ابزار تشخیص چهره مانند Face++ نیز استفاده کنم که به شما این امکان را می‌دهد که دو عکس را بارگذاری کنید و سپس احتمال اینکه آن‌ها متعلق به یک شخص باشند را به‌صورت درصد نمایش می‌دهد. در این نمونه‌ها، این ابزار توانست من را در عکس‌هایی که با فاصله ۱۰ سال گرفته شده بودند با موفقیت شناسایی کند. همچنین این ابزار توانست عکس‌های همکارم بن را در شبکه‌های اجتماعی از جمله توئیتر و فیس‌بوک شناسایی کند و درعین‌حال تشخیص دهد که او در واقع بن استیلر (هنرپیشه‌ی آمریکایی) نیست.



اگر در حال تعقیب ترول‌های فضای مجازی و یا کلاهبرداران هستید، احتمالا متوجه خواهید شد که

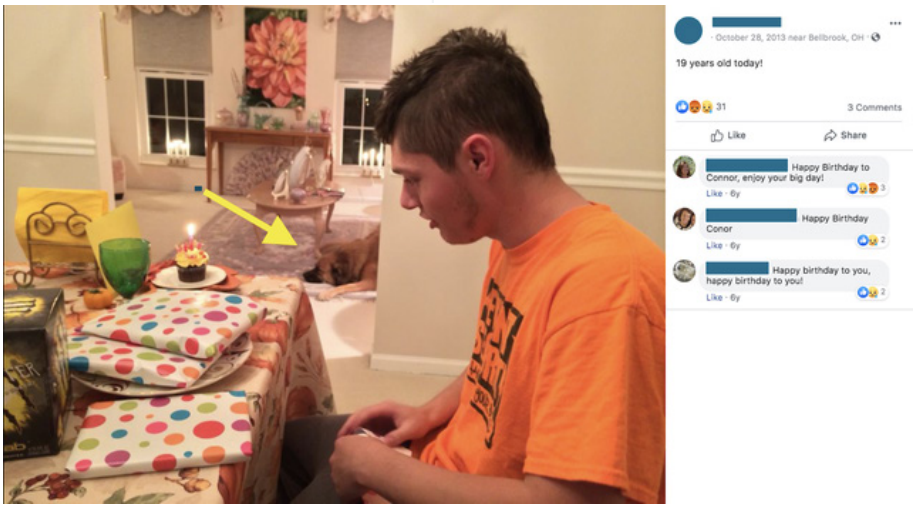
آن‌ها تلاش بیشتری را صرف محو و نامشخص کردن عکس‌های خود کرده و یا از عکس‌های غیرواقعی و جعلی استفاده می‌کنند. بنابراین معکوس کردن ویرایش‌هایی که روی عکس‌ها صورت گرفته می‌تواند به مهندسی معکوس روش آن‌ها کمک کند.

بااین‌حال، فقط عکس‌های حساب‌های کاربری نیستند که می‌توانند راهنمای ما باشند. با اینکه افراد امروزه بیش از پیش به حفظ حریم خصوصی خود و خانواده‌شان حساس هستند و به آن اهمیت می‌دهند، اما همچنان تمایل دارند عکس‌هایی از چیزهایی که به آن افتخار می‌کنند به اشتراک بگذارند. من موفق شده‌ام افراد را با ارتباط دادن عکس‌هایی از خانه‌ها، ماشین‌ها و حیوانات خانگی شناسایی کنم. از این منظر، عکس‌ها به وسیله‌ای برای اتصال حساب‌ها و افرادی که پشت آن‌ها پنهان شده‌اند، تبدیل می‌شوند و شما را قادر می‌سازند که شبکه‌ای اطراف هدف خود ایجاد کنید. این یکی از روش‌های اصلی به هنگام بررسی حساب‌های رسانه‌های اجتماعی است.

به‌عنوان مثال، ما به دنبال تأیید حساب‌های کاربری مردی بودیم که ۹ نفر را بیرون یک بار در دیتون، اوهایو به ضرب گلوله کشته بود. حساب توئیتر او سرنخ‌هایی از ایدئولوژی سیاسی او به دست می‌داد، اما نام کاربری‌اش، @iamthespookster، منحصربه‌فرد بود و به نام واقعی او که توسط مقامات منتشر شده بود، شباهتی نداشت. این واقعیت که یکی از قربانیان او برادرش بود -مردی تراجنسیتی که مشخصاتش در سوابق عمومی وجود نداشت و هنوز هویت جدیدش را برای عموم فاش نکرده بود- شناسایی سرنخ‌ها را دشوارتر می‌کرد. اما همه جا در عکس‌های خود او و خانواده‌اش تصاویری از یک سگ وجود داشت و این

راهنمایی بود که ما را به حساب کاربری گزارش‌نشده‌ی برادر تراجنسیتی راهنمایی کرد.

اما در تصویر بالا سگ خانگی تنها سرنخ موجود نبود. این عکس که از پدر تیرانداز اوهایو به دست آمده بود و به ما کمک کرد حساب‌های کاربری او و اعضای خانواده‌اش را تأیید کنیم.



اگر در فیس‌بوک یا توئیتر حساب کاربری داشته باشید، احتمالا خواهم توانست تاریخ تولدتان را پیدا کنم، حتی اگر آن را در بخش «درباره‌ی من» در حساب کاربری خود ذکر نکرده باشید. از آنجایی که تاریخ تولد یکی از اولین اطلاعاتی است که در موقعیت‌های خبری فوری توسط پلیس کشف و ارائه می‌شود، یک راه مطمئن برای تأیید حساب کاربری رسانه‌های اجتماعی این است که به ماه و روز مورد نظر در حساب مشکوک بروید و به دنبال تبریک‌های تولد بگردید. حتی اگر در صفحه‌ی خود فرد اطلاعاتی وجود نداشته باشد، پدر و مادرها (مانند کانر بتز در تصویر بالا) اغلب مطلبی درباره‌ی تولد فرزندانشان به اشتراک می‌گذارند.

همین امر در مورد توئیتر هم صادق است، چرا که کیست که عاشق روز تولد نباشد؟!

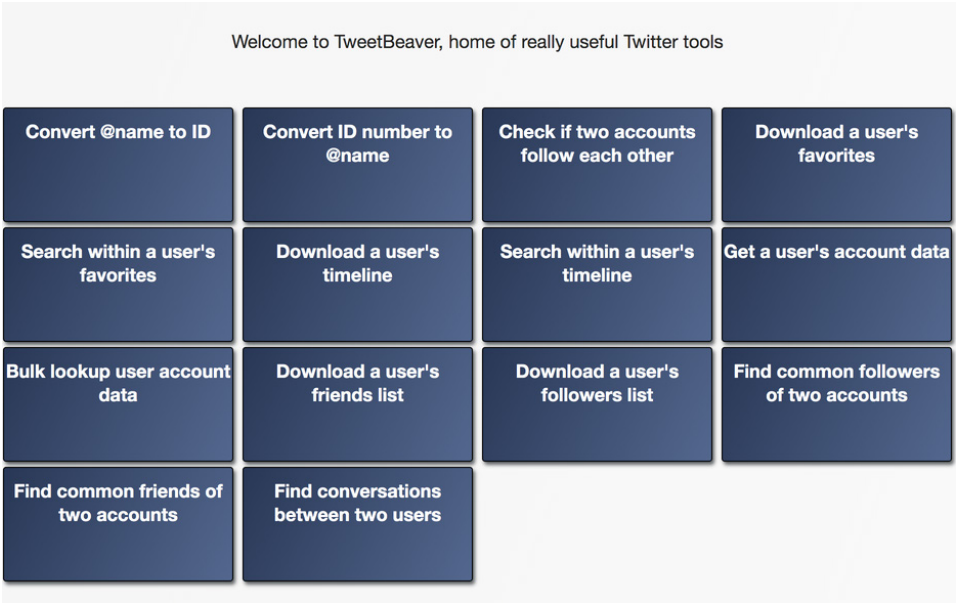
اما یافتن پستی که شناسایی فرد را ممکن کند در توئیتر حتی آسان‌تر نیز هست، زیرا ابزار جستجوی پیشرفته‌ی آن یکی از بهترین‌هایی است که توسط پلتفرم‌های اجتماعی ارائه می‌شود. اگرچه من به ندرت تولدم را اعلام می‌کنم، موفق شدم تبریکی که یک همکار بامحبت برای روز تولدم روی توئیترم پست کرده بود پیدا کنم که تاریخ تولدم را برملا می‌کرد.

تولد فقط یک مثال است. عروسی‌ها، ترحیم‌ها، تعطیلات، سالگردها، فارغ التحصیلی‌ها - تقریباً همه‌ی اتفاقات مهم زندگی در رسانه‌های اجتماعی جشن گرفته یا یادآوری می‌شوند. همه‌ی این‌ها فرصتی برای جستجو و بررسی یک حساب کاربری را فراهم می‌کنند. می‌توانید برای جستجو از این کلیدواژه‌ها یا فیلترهای دیگر ابزارهای جستجوی فیس‌بوک استفاده کنید. شاید ابزارها دیگر به اندازه‌ی زمانی که پلتفرم‌ها اقدامات جدید مربوط به حریم خصوصی را اعمال نکرده بودند کارآمد نباشند، اما هنوز هم کار می‌کنند. یکی از ابزارهای مورد علاقه‌ی من whopostedwhat.com است.

روابط

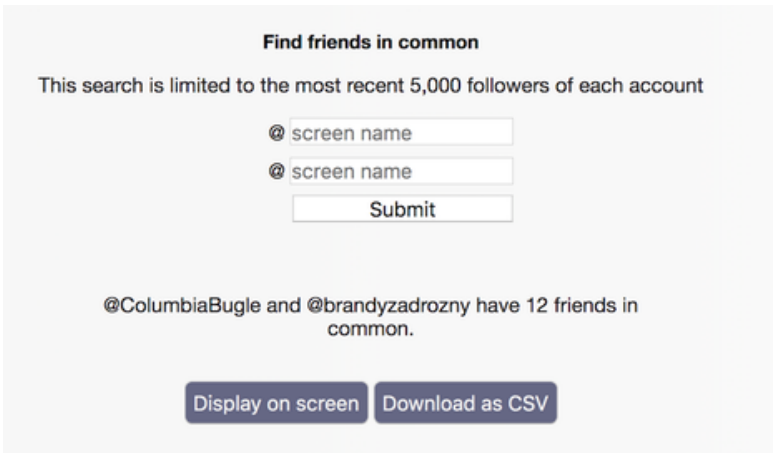
شما می‌توانید یک شخص را بر اساس معاشرانی که در شبکه‌های اجتماعی دارد قضاوت کنید. با بررسی افرادی که سوژه‌ی مورد نظرمان با آن‌ها به صورت آنلاین ارتباط برقرار می‌کنند، می‌توانیم چیزهای زیادی درباره‌ی زندگی و تمایلاتش کشف کنیم.

وقتی برای اولین بار به توئیتر ملحق شدم، شوهر و بهترین دوستم را نیز وادار به ثبت نام کردم تا بتوانند من را دنبال کنند. بنابراین در کارم هم وقتی به دنبال حساب‌های کاربری هستم، به این موضوع فکر می‌کنم. پلتفرم‌ها هم نمی‌خواهند شما تنها باشید، بنابراین وقتی برای اولین بار حساب باز می‌کنید، یک الگوریتم فعال می‌شود. با توجه به فهرست مخاطبان در تلفن شما، حضور شما در فهرست مخاطبین حساب‌های کاربری موجود، موقعیت مکانی‌تان و سایر عوامل، پلتفرم حساب‌هایی را برای دنبال کردن به شما پیشنهاد می‌کند. به همین دلیل همیشه بررسی اولین دنبال‌کننده‌ها و دوستان یک کاربر می‌تواند نکات زیادی را روشن کند. TweetBeaver ابزار خوبی برای بررسی ارتباط بین حساب‌های بزرگ و دانلود مواردی مانند تایم‌لاین‌ها و موضوعات محبوب حساب‌های کاربری کوچک‌تر است. برای مجموعه‌داده‌های بزرگ‌تر، من به توسعه‌دهنده‌ای (Developer) با دسترسی API متکی هستم.

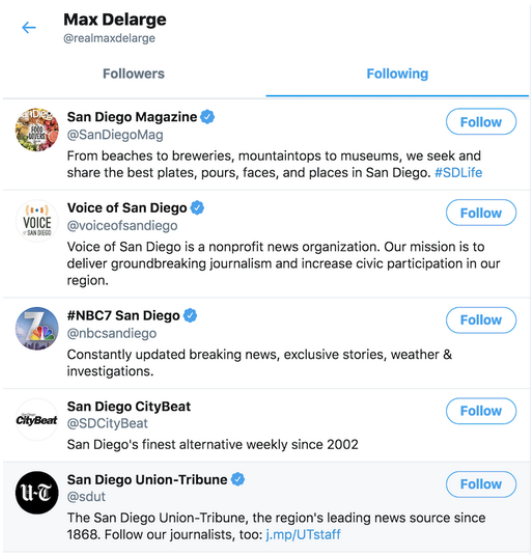


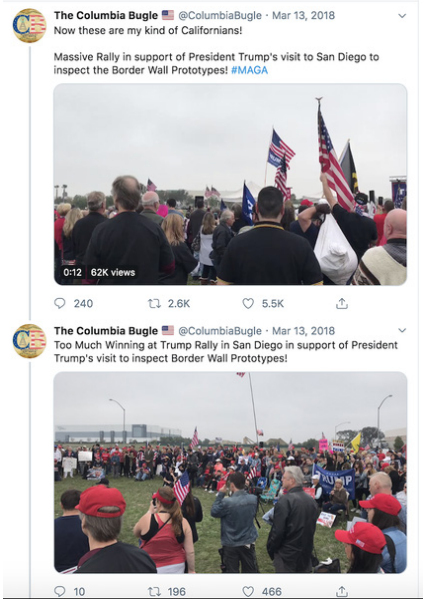
اجازه بدهید به‌عنوان مثال The Columbia Bugle را در نظر بگیریم، یک حساب کاربری ناشناس راست افراطی محبوب در توئیتر که به خود می‌بالد دو بار توسط دونالد ترامپ ریتوییت شده است.

اولین دنبال‌کننده‌های مکس دِلارج، حساب کاربری‌ای که ادعا می‌کند ویراستار The Columbia Bugle است منابع خبری و حساب‌های ورزشی مختص سن‌دیه‌گو هستند. از آنجایی که بسیاری از توئیت‌های کلمبیا بیوگل شامل ویدئوهایی از تظاهرات و رویدادهای انتخاباتی ترامپ در دانشگاه کالیفرنیا، سن‌دیه‌گو است، می‌توانیم کاملاً مطمئن باشیم که شخصی که پشت این حساب کاربری است در نزدیکی سن‌دیه‌گو زندگی می‌کند.



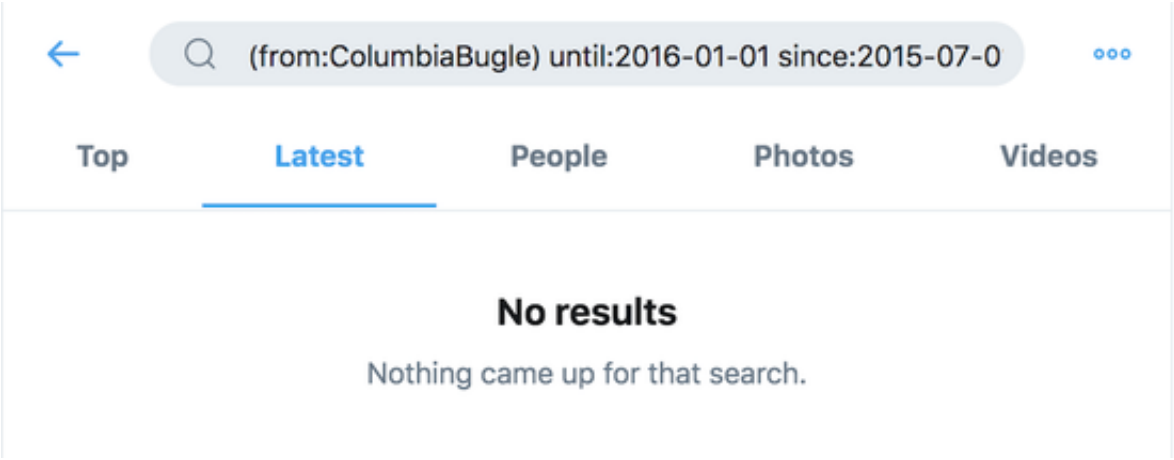

Follow
Max Delarge
@realMaxDelarge
Co-Editor of The Columbia Bugle. Still got the scars of #NeverTrump, but im on the #TrumpTrain for good, unless he lights the train on fire
United States
Joined July 2016
22 Following
0 Followers


Max Delarge
@realmaxdelarge
Followers
Following
San Diego Magazine
@SanDiegoMag
Follow
From beaches to breweries, mountaintops to museums, we seek and share the best plates, pours, faces, and places in San Diego. #SDLife
Voice of San Diego
@voiceofsandiego
Follow
Voice of San Diego is a nonprofit news organization. Our mission is to deliver groundbreaking journalism and increase civic participation in our region.
#NBC7 San Diego
@nbcsandiego
Follow
Constantly updated breaking news, exclusive stories, weather & investigations.
San Diego CityBeat
@SDCityBeat
Follow
San Diego's finest alternative weekly since 2002
San Diego Union-Tribune
@sdut
Follow
The San Diego Union-Tribune, the region's leading news source since 1868. Follow our journalists, too: j.mp/UTstaff


The Columbia Bugle @ColumbiaBugle · Mar 13, 2018
Now these are my kind of Californians!
Massive Rally in support of President Trump's visit to San Diego to inspect the Border Wall Prototypes! #MAGA
0:12 62K views
240
2.6K
5.5K
The Columbia Bugle @ColumbiaBugle · Mar 13, 2018
Too Much Winning at Trump Rally in San Diego in support of President Trump's visit to inspect Border Wall Prototypes!
10
196
466

برای هر تحقیق جدید من ترجیح می‌دهم از ابتدای تاریخچه‌ی توئیتر شخص شروع کنم و قدم‌به‌قدم جلو بروم. می‌توانید این کار را دستی انجام بدهید یا از یک افزونه‌ی Chrome autoscroller استفاده کنید و یا از گزینه‌ی جستجوی پیشرفته‌ی توئیتر برای محدود کردن بازه‌ی زمانی به اولین ماه‌های ایجاد حساب کاربری استفاده کنید.

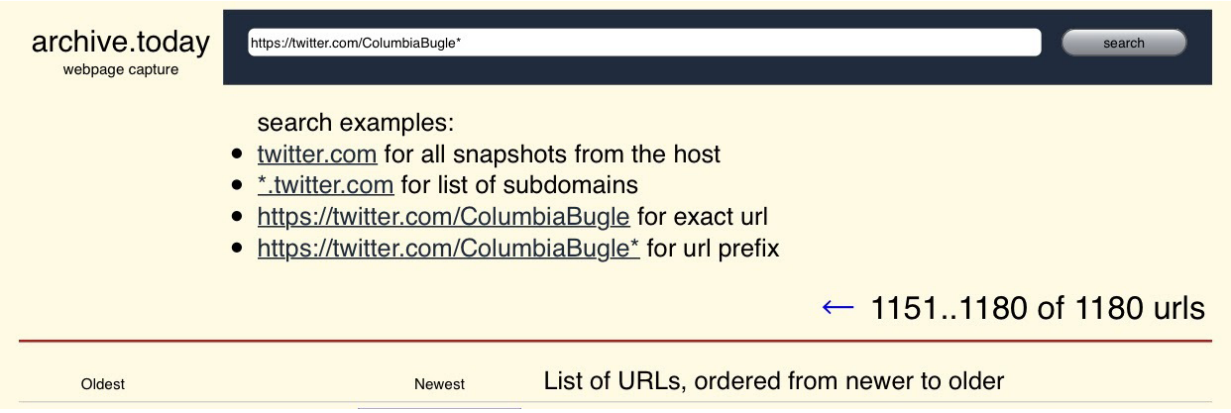
جالب است که در شش ماه اول بعد از ایجاد این حساب کاربری هیچ توئیتی وجود ندارد.

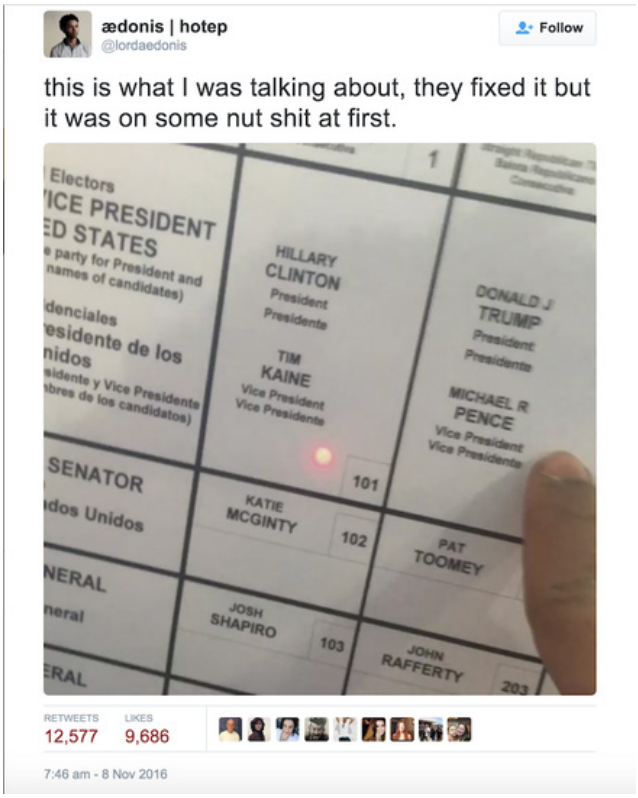


این بدین معنا است که صاحب این حساب کاربری ممکن است اولین توئیت‌های خود را حذف کرده باشد. برای فهمیدن دلیل آن می‌توانم جستجوی خود را کمی تغییر بدهم؛ به جای توئیت‌های خود حساب کاربری به دنبال هر توئیتی می‌گردم که به کلمبیا بیوگل اشاره می‌کند.

این مکالمات نشان می‌دهند کلمبیا بیوگل توئیت‌هایی را که در اولین سال فعالیت خود زده حذف کرده است اما برای فهمیدن دلیل آن کمکی نمی‌کند. اولین حساب‌هایی که کلمبیا بیوگل با آن‌ها تعامل داشته نیز سرنخ چندانی به دست نمی‌دهند.

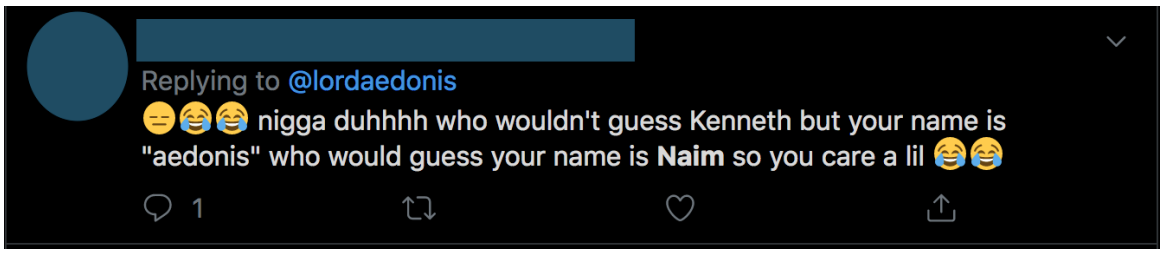
برای پیدا کردن توئیت‌هایی که اخیرا حذف شده‌اند می‌توانید حافظه‌ی نهان (cache) گوگل را جستجو کنید. توئیت‌های حذف‌شده‌ی قدیمی‌تر را نیز می‌توان گاهی در Internet Archive's Wayback Machine یا آرشیوهای دیگر پیدا کرد. سایت آرشیو دستی archive.is چندین توئیت حذف‌شده از کلمبیا بیوگل مربوط به رویدادی را نشان می‌دهد که در آن شرکت کرده بود؛ در این رویداد دانشجویان طرفدار ترامپ پیام‌هایی را در محوطه دانشگاه خود نوشته بودند. برای دیدن همه توئیت‌هایی که شخصی از حساب کاربری خود بایگانی کرده، می‌توانید همان کاری را بکنید که من برای پیدا کردن این توئیت انجام دادم: استفاده از پیشوند URL به اضافه‌ی یک ستاره که بعد از نام حساب کاربری قرار می‌گیرد، مانند شکل زیر:





به‌ندرت پیش می‌آید که کسی بتواند فعالیت‌های آنلاین خود را کاملا از زندگی واقعی‌اش جدا نگه دارد. به‌عنوان مثال، من و همکارم در ان‌بی‌سی‌نیوز داستان پربازدیدترین - و گمراه‌کننده‌ترین- ادعای تقلب در روز انتخابات ۲۰۱۶ را نقل کردیم و برای این کار از آشنای هم‌محلی ترول راست افراطی‌ای که توئیت را ارسال کرده بود کمک گرفتیم.

اگرچه این توئیت توسط مردی ارسال شده بود که برای دنبال‌کنندگانش به نام @lordaedonis شناخته می‌شد، اما هم‌محله‌ای‌های واقعی او به توئیت‌های گذشته‌اش با نام واقعی او پاسخ داده بودند و به این ترتیب مشخص شد حساب کاربری متعلق به یک کارآفرین تشنه‌ی توجه است که توئیتش توسط یک حساب توییتری نزدیک به کرملین منتشر شده بود و در نهایت توسط میلیون‌ها نفر دیده شد و توسط رئیس جمهور آینده هم تبلیغ شده بود.

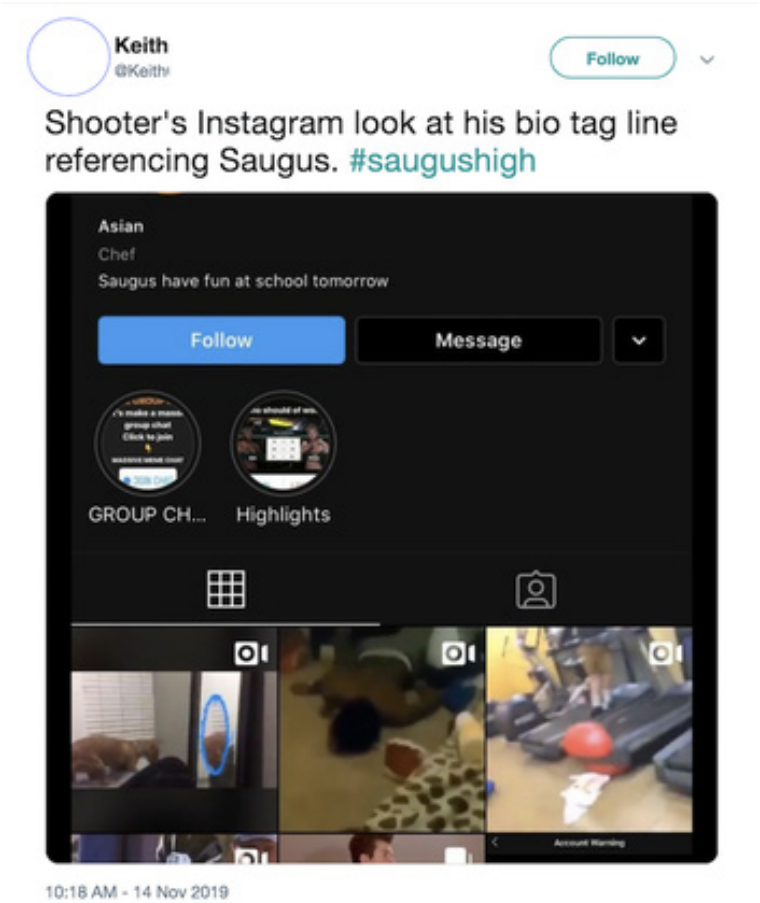


داستان‌های مورد علاقه‌ی من آن‌هایی هستند که هویت افراد واقعیِ پشت حساب‌های ناشناس و تأثیرگذار در شبکه‌های اجتماعی را برملا می‌کنند. این حساب‌های مخفی کمتر به الگوریتم وابسته هستند و با دقت بیشتر برای فرار از زندگی عمومی ساخته شده‌اند. این حساب‌های کاربری به صاحبان خود این امکان را می‌دهند که جدا از حساب عمومی خود، با خانواده و دوستان خود تماس داشته باشند و با آن‌ها ارتباط برقرار کنند، یا عقاید و نظراتی را که به دلایل شخصی یا سیاسی جرأت نمی‌کنند با صدای بلند بیان کنند، در میان بگذارند.

روزنامه‌نگار اشلی فاینبرگ استاد این نوع داستان‌های جالب و جنجالی است؛ داستان‌هایی که حساب‌های کاربری مستعار افراد سرشناسی مثل جیمز کومی یا میت رامنی را برملا می‌کنند. شگرد کار او ساده بود؛ ابتدا حساب‌های کاربری کوچک‌تر متعلق به اعضای خانواده را که کومی یا رامنی طبیعتا می‌خواستند دنبال کنند را پیدا می‌کرد. سپس در این حساب‌ها می‌گشت تا حساب کاربری‌ای را پیدا کند که غیرواقعی به نظر می‌رسید اما محتوا و شبکه‌ی دوستان/دنبال‌کنندگان آن با این اشخاص واقعی مطابقت داشت.

مراقب حساب‌های جعلی باشید

هر پلتفرمی، شخصیت، قابلیت‌های جستجو و عناصر مفید خود را در موقعیت‌های خبری گوناگون دارد. اما یک هشدار کوچک درباره‌ی حساب‌های کاربری شبکه‌های اجتماعی: قاعده‌ی همیشگی «اطمینان کنید اما تحقیق و تأیید کنید» در مورد آن‌ها نیز صادق است. گروه‌های مختلفی از افراد از حقه زدن به خبرنگاران لذت می‌برند. خاصه در موقعیت‌های خبری فوری همیشه حساب‌های کاربری جعلی‌ای متولد می‌شوند و بسیاری از آن‌ها برای جذب خبرنگاران مطالب شوم و تهدیدآمیزی را به اشتراک می‌گذارند. یک حساب کاربری جعلی در اینستاگرام از نام فردی استفاده کرده بود که چندین تن را به ضرب گلوله در دبیرستان ساوگوس در کالیفرنیا کشته بود. حساب کاربری بعد از ماجرای تیراندازی ایجاد شده بود و از طریق اسکرین‌شات‌هایی که از آن در توئیتر منتشر شده بود توجه عموم را به خود جلب کرد. اما بعدتر سایت بازفید فاش کرد که حساب درواقع متعلق به ضارب مدرسه‌ی ساوگوس نیست. تأیید حساب‌های کاربری شبکه‌های اجتماعی با موضوع، خانواده و دوستان، مجریان قانون و یا روابط عمومی رسانه‌های اجتماعی راه‌هایی برای محافظت از خود در برابر فریب خوردن هستند.



آخرین، و شاید مهم‌ترین نکته اینکه: تنها یک ترتیب درست برای تکمیل این مراحل وجود ندارد. من اغلب گرفتار گرداب‌های فضای مجازی می‌شوم و تعداد صفحاتی که در

جستجوگرم باز کرده‌ام آن‌قدر زیاد می‌شود که خجالت‌آور است. ایجاد سیستمی تکرارپذیر -به‌عنوان مثال ثبت کردن مراحل در Google doc یا استفاده از یک ابزار پولی مانند Hunchly که قدم‌هایتان را در حین جستجو ثبت کند- می‌تواند به روشن کردن ارتباط بین افراد و زندگی‌ای که در فضای مجازی دارند کمک کند و نتایج تحقیقاتتان را به یک داستان کامل تبدیل کند.

۱.الف. مطالعه‌ی موردی: چگونه بررسی تعدادی حساب کاربری در فیس‌بوک از تلاشی هماهنگ برای گسترش پروپاگاندا در فیلیپین پرده برداشت.

نوشته‌ی: **ورنیس تانتوکو و جما باگایاو-مندوزا**

جما باگایاو-مندوزا با بیش از ۲۰ سال سابقه‌ی خبرنگاری حرفه‌ای، مدیر تحقیقات و استراتژی در شرکت رسانه‌ای راپلر است. او واحد بررسی حقایق را راهبری می‌کند و همچنین مدیریت تحقیقات راپلر در مورد دروغ‌پراکنی در فضای مجازی و اطلاعات نادرست را نیز بر عهده دارد.

ورنیس تانتوکو یکی از اعضای تیم تحقیقاتی راپلر است و کار او صحت‌سنجی و مطالعه‌ی شبکه‌های اطلاعات نادرست در فیلیپین است.

در پاییز سال ۲۰۱۶، جان ویکتورینو، یک تحلیلگر سرمایه‌گذاری، فهرستی از ۲۶ حساب کاربری مشکوک فیس‌بوک در فیلیپین را برای راپلر ارسال کرد. ما شروع به بررسی و رصد حساب‌ها کردیم و به سرعت متوجه شدیم که جزئیات ذکرشده در پروفایل آن‌ها نادرست است. در طول هفته‌ها تحقیق، این ۲۶ حساب ما را به سمت کشف شبکه‌ی بسیار گسترده‌تری از صفحات، گروه‌ها و حساب‌ها سوق دادند.

این حساب‌ها به همراه مجموعه‌ای از صفحات و گروه‌هایی که به آن‌ها متصل بودند، در نهایت توسط فیس‌بوک حذف شدند. کشف این شبکه از حساب‌ها همچنین مشوق راپلر برای طراحی Sharktank بود، ابزاری برای نظارت بر جریان اطلاعات در فیس‌بوک. این کار همچنین اساس مجموعه‌ای از تحقیقات در مورد چگونگی تأثیر عملیات تبلیغاتی و اطلاعاتی در فیس‌بوک بر دموکراسی در فیلیپین را نیز تشکیل داد. این مجموعه شامل تحقیق در مورد فعالیت‌های ۲۶ حساب جعلی و آغازگر پوشش مداوم ما از نحوه‌ی استفاده از فیس‌بوک در فیلیپین برای انتشار اطلاعات نادرست سیاسی، آزار و اذیت افراد و تضعیف دموکراسی در این کشور بود.

در این مطالعه‌ی موردی نگاهی خواهیم انداخت به نحوه‌ی انجام تحقیقات در مورد این ۲۶ حساب کاربری و استفاده از آن برای کشف شبکه‌های بسیار بزرگ‌تر.

تأیید هویت، افشای حساب‌های جعلی

اولین قدم ما در بررسی مجموعه حساب‌ها بررسی این موضوع بود که آیا این صفحات به افراد واقعی متصل هستند یا خیر. این بخش مستلزم بررسی با استفاده از شیوه‌های سنتی راستی‌آزمایی بود و با ایجاد صفحات گسترده‌ای برای ردیابی جزئیات مربوط به حساب‌ها، از جمله جزئیات شخصی‌ای که در آن‌ها ذکر شده بودند، صفحاتی که لایک کرده بودند و سایر اطلاعات شروع شد.

به‌عنوان مثال، یکی از این کاربران به نام موتیا باوتیستا خود را «تحلیلگر نرم‌افزار» در اِی‌بی‌اس-سی‌بی‌ان، بزرگترین شبکه‌ی تلویزیونی فیلیپین توصیف کرده بود. راپلر با اِی‌بی‌اس-سی‌بی‌ان تماس گرفت و آن‌ها تأیید کردند که فردی به این نام در این شبکه کار نمی‌کند.

Personal Information	
Facebook ID	https://www.facebook.com/profile.php?id=10
Profile Name	Mutya Bautista
Occupation	Software Analyst
Current Company	ABS-CBN Corporation
Former Occupation 1	
Former Occupation 2	
Former Occupation 3	
Former Occupation 4	
Former Occupation 5	
Studied	Computer Engineering
Studied at	University of the Philippines
Went to	
Lives in	
Married to	
From	
Account Set-up Date	October 19, 2015

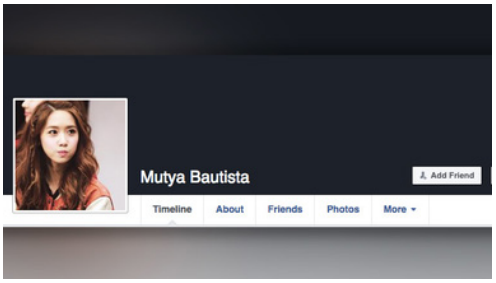
Liked Pages	Liked Pages Facebook ID
Okay Dito	https://www.facebook.com/vidtimestories/
The Philippine Pride	https://www.facebook.com/sirangplaka2/

Photos	Source of Photo
Profile Photo	Numerous sources. Im Yoona of SNSD
Cover Photo	

با استفاده از ابزارهای جستجوی معکوس عکس، متوجه شدیم که بسیاری از این ۲۶ حساب کاربری از عکس‌های افراد و شخصیت‌های مشهور برای پروفایل خود استفاده می‌کنند.

برای مثال، باوتیستا از تصویر ایم یونا، عضو گروه پاپ کُره‌ای گرلز جنریشن استفاده کرده بود.

حساب کاربری لیلی لوپز که در زیر نشان داده شده است، از تصویر بازیگر کره‌ای کیم سا-رانگ استفاده کرده است.



حساب دیگری با نام کاربری لوویمین کانسیو از تصویری از softcorecams.com، یک سایت پورنوگرافی، به‌عنوان عکس پروفایل خود استفاده کرده بود. منبع عکس را از طریق ابزار جستجوی معکوس TinEye شناسایی کردیم.

این حساب‌ها همچنین از عکس‌های مشابهی برای کاورفوتوی خود استفاده می‌کردند. در زیر، عکس کاور حساب کاربری یاسمین ده‌لاتوره با لیلی لوپز یکی است.

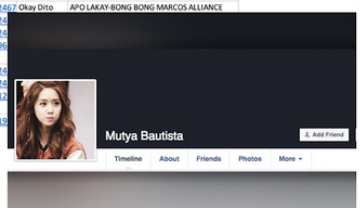
ما همچنین متوجه یک موضوع عجیب دیگر در مورد این ۲۶ حساب کاربری شدیم: تعداد گروه‌های این کاربران عضو آن بودند بیشتر از تعداد دوستانشان در فیس‌بوک بود.

این غیرعادی بود، زیرا در فیلیپین اکثر مردم تعدادی دوست و اعضای خانواده در خارج از کشور دارند. فیس‌بوک اساسا به‌عنوان کانال ارتباطی برای تماس با خانواده و دوستان عمل می‌کند. بنابراین، بیشتر افراد تعداد زیادی دوست دارند و تعداد دوستانشان در مقایسه با گروه‌هایی که در آن‌ها عضو هستند بسیار بیشتر است.

فهرست دوستان باتیستا (که در آن زمان عمومی بود) نشان می‌داد که او تنها ۱۷ دوست دارد. درواقع، در سال ۲۰۱۶ و به هنگام کشف این حساب‌ها، هرکدام کمتر از۵۰ دوست داشتند.

با این حال، باوتیستا عضو بیش از صد گروه بود، از جمله گروه‌هایی که برای فردیناند مارکوس جونیور (که آن زمان نامزد معاونت ریاست‌جمهوری بود) تبلیغ می‌کردند، تعدادی از جوامع فیلیپینی‌های خارج از کشور، و همچنین گروه‌های خرید و فروش، که تعداد اعضای هرکدام بین ده‌ها تا صدها هزار تن بود. در مجموع، این گروه‌ها بیش از ۲.۳ میلیون عضو در فیس‌بوک داشتند. در ادامه فهرستی از برخی از بزرگ‌ترین گروه‌ها و تعداد دنبال‌کننده‌های آن‌ها آمده است. همچنین فهرستی از پست‌هایی که باوتیستا برای این گروه‌ها ارسال کرده نیز آورده شده است.

GROUPS JOINED			CONTENT POSTED			
Group URL	Group Name	Group Members	DATE POSTED	Posts	Source	Group
https://www.facebook.com/groups/7551643712	Tambayan ng mga maranao samok 15	512,164		https://www.facebook.com/groups/321991	Okay Dito	We Support Bongbong Marcos
https://www.facebook.com/groups/bbmunited/	BongBong Marcos United	156,267	August 8, 2016	https://www.facebook.com/groups/166036	Okay Dito	OFW,KASABONG,KAIBIGAN GROUP
https://www.facebook.com/groups/5774321323	DOG LOVERS PHILIPPINES	133,437	August 5, 2016	https://www.facebook.com/groups/107711	Okay Dito	BABANGON AKO PARA SA PAGKAKAISA SOLID BONGBONG MARCOS GROUP (CAMANAVA AREA)
https://www.facebook.com/groups/OFWnewgen	ON-LINE FILIPINO WORKER (OFW)	56,067	July 29, 2016	https://www.facebook.com/groups/166036	Okay Dito	OFW,KASABONG,KAIBIGAN GROUP
https://www.facebook.com/groups/6474477453	PINOY OFW SA UAE (Overseas Filipino W	53,169	July 29, 2016	https://www.facebook.com/groups/321991	Okay Dito	We Support Bongbong Marcos
https://www.facebook.com/groups/2042054097	Pinoy Networkers - Ads Center for Every	44,773	July 25, 2016	https://www.facebook.com/groups/102468	Okay Dito	Pro Bongbong Marcos International Power
https://www.facebook.com/groups/morefunphil	It's MORE FUN in the PHILIPPINES	44,339	July 24, 2016	https://www.facebook.com/groups/166036	Okay Dito	OFW,KASABONG,KAIBIGAN GROUP
https://www.facebook.com/groups/CAVITE.SALE	CAVITE SALES,TRADE,SWAP motorcycle g	42,147	July 24, 2016	https://www.facebook.com/groups/112467	Okay Dito	APO LAKAY-BONG BONG MARCOS ALLIANCE
https://www.facebook.com/groups/pinoyofwsec	PINOY OFW'S MEETING SECTION	38,950	July 18, 2016	https://www.facebook.com/groups/112467	Okay Dito	APO LAKAY-BONG BONG MARCOS ALLIANCE
https://www.facebook.com/groups/3481705587	Online Business For Filipinos Worldwide	38,202	July 17, 2016	https://www.facebook.com/groups/102468	Okay Dito	Pro Bongbong Marcos International Power
https://www.facebook.com/groups/mgafilipinos	Mga Filipino sa United Kingdom	33,740	July 16, 2016	https://www.facebook.com/groups/102468	Okay Dito	Pro Bongbong Marcos International Power
https://www.facebook.com/groups/ofw.globalkı	Ofw sa kuwait	33,569	June 25, 2016	https://www.facebook.com/groups/102468	Okay Dito	Pro Bongbong Marcos International Power
https://www.facebook.com/groups/entrepinoy/	PINOY AFFILIATE Marketing BUSINESS	33,199	June 16, 2016	https://www.facebook.com/groups/102468	Ask Philippine	Pro Bongbong Marcos International Power
https://www.facebook.com/groups/3691104898	Pinoy Tambayan Ads Qatar	29,520	May 24, 2016	https://www.facebook.com/groups/112467	Okay Dito	APO LAKAY-BONG BONG MARCOS ALLIANCE
https://www.facebook.com/groups/1505766333	Jobs hiring in lipa area/tanauan area/bat	28,212	May 18, 2016	https://www.facebook.com/groups/Bongbc	Okay Dito	SenaThorBongbongMarcosGroupPage_TeamKulit
https://www.facebook.com/groups/1458352404	Pinoy OFW in Malaysia..	26,076	May 17, 2016	https://www.facebook.com/groups/321991	Okay Dito	We Support Bongbong Marcos
https://www.facebook.com/groups/1921370942	Buy Sell Barter Philippines	25,888	May 17, 2016	https://www.facebook.com/groups/112467	Okay Dito	APO LAKAY-BONG BONG MARCOS ALLIANCE
https://www.facebook.com/groups/mgafilipinos	Mga Filipino sa China	25,128	May 17, 2016	https://www.facebook.com/groups/247154	Okay Dito	BONGBONG MARCOS FOR BETTER & GREATER PHILIPPINES 2016
https://www.facebook.com/groups/1619426761	TAMBAYAN NG MGA NAGHAHANAP NG T	24,387	May 16, 2016	https://www.facebook.com/groups/112467	Okay Dito	APO LAKAY-BONG BONG MARCOS ALLIANCE
https://www.facebook.com/groups/swapphilipp	SWAP!!! PHILIPPINES	24,363	May 13, 2016	https://www.facebook.com/groups/1124		
https://www.facebook.com/groups/mgafilipinos	Mga Filipino sa Hong Kong	24,325	May 8, 2016	https://www.facebook.com/groups/1024		
https://www.facebook.com/groups/mgafilipinos	Mga Filipino sa Japan	23,803	May 7, 2016	https://www.facebook.com/groups/1196		
https://www.facebook.com/groups/mgafilipinos	Mga Filipino sa Spain	22,761	May 6, 2016	https://www.facebook.com/groups/1024		
https://www.facebook.com/groups/4823165519	SAMAHAN NG MAKUKULIT NA OFW 2	22,745	May 5, 2016	https://www.facebook.com/groups/1024		
https://www.facebook.com/groups/LDSERCPhili	LDS Employment Resource Center- Philij	22,711	May 5, 2016	https://www.facebook.com/groups/6812		
https://www.facebook.com/groups/sellsomethir	SELL SOMETHING PHILIPPINES	21,504	May 5, 2016	https://www.facebook.com/groups/3219		



با ترکیب همه‌ی این مشاهدات و داده‌های مرتبط، به این نتیجه رسیدیم که حساب‌ها از نوع حساب‌های کاربری زاپاس هستند: هویت‌های ساختگی ایجاد شده برای تقویت یک دیدگاه خاص.

شبکه‌ی حامیان مارکوس

از روی تاریخ اولین عکس‌ها و پست‌های این ۲۶ حساب‌های کاربری می‌شد فهمید که حساب‌ها در فاصله‌ی زمانی ربع آخر سال ۲۰۱۵ تا انتخابات ماه مه سال ۲۰۱۶ ساخته شده‌اند. همچنین دریافتیم که این حساب‌ها پیوسته محتواهایی را تبلیغ می‌کردند که سوءاستفاده از قوانین حکومت نظامی در دهه‌ی ۱۹۷۰ که در رژیم مارکوس رخ داده بودند را انکار می‌کردند. آن‌ها همچنین مرتب به رقبای پسر دیکتاتور سابق و نامزد معاونت ریاست‌جمهوری، فردیناند «بونگ‌بونگ» مارکوس جونیور نیز حمله می‌کردند.

در مثال زیر، حساب کاربری موتیا باوتیستا ادعای (اکنون ردشده‌ای) را به اشتراک گذاشته بود که می‌گفت یکی از رقبای بونگ‌بونگ به نام لنی ربردو (که آن زمان تازه به‌عنوان معاون رئیس‌جمهور انتخاب شده بود) قبل از ازدواج با همسر دوم خود، جس روبردوی فقید (وزیر کشور دولت محلی)، همسر یک کنشگر سیاسی بوده است. باتیستا این داستان را با تیتر «لنی روبردو قبل از ملاقات با جسی با یک نوجوان مخالف مارکوس ازدواج کرده بود؟» در گروه قدرت بین‌المللی حامیان بونگ‌بونگ مارکوس پست کرده بود و در قسمت نظرات نوشته بود: «برای همین است که قضیه [علیه بونگ بونگ مارکوس] شخصی است. مشکل از جای دیگری آب می‌خورد».

حساب مشکوک دیگری با نام رادن آلفارو پایاس، همان مقاله را با همان شرح -کلمه به کلمه، تا آخرین نقطه‌گذاری و در همان روز در گروه «جنگجویان وفادار بونگ‌بونگ مارکوس در فیس‌بوک» به اشتراک گذاشته بود.

اغلب برای فرستادن لینک هرزنامه به گروه‌ها از حساب‌های کاربری جعلی استفاده می‌شود. گاهی اوقات چند حساب کاربری جعلی ممکن است از متن یکسانی برای این کار استفاده کنند. در آن زمان، امکان استفاده از جستجوی Facebook Graph برای مشاهده‌ی پست‌های عمومی کاربران در گروه‌ها وجود داشت. اما فیس‌بوک بسیاری از گزینه‌های جستجوی Graph، از جمله این گزینه، را در سال ۲۰۱۹ مسدود کرد. درنتیجه، در حال حاضر لازم است به گروه‌ها بروید و جستجو کنید تا ببینید کاربران خاص چه چیزهایی را به اشتراک گذاشته‌اند.

وب‌سایت‌های متصل

با تجزیه و تحلیل محتوای به اشتراک گذاشته شده توسط این ۲۶ حساب کاربری، متوجه شدیم که تمام این حساب‌های جعلی وب‌سایت‌های یکسانی را تبلیغ می‌کنند، از جمله:

why0why.com، Ask Philippines (askphilippines.com)، Okay Dito (OKD2.com) و غیره.

OKD2.com تعدادی مطالب دروغین و مطالب تبلیغاتی به نفع خانواده‌ی مارکوس و رئیس‌جمهور رودریگو دوترته منتشر کرده است. این سایت اکنون در پوشش ظاهری یک سایت تبلیغات طبقه‌بندی‌شده فعالیت می‌کند. اما متوجه شدیم که در سپتامبر سال ۲۰۱۶ و به کمک حساب‌های کاربری جعلی مطالب این وب‌سایت ۱۱۹۰۰ بار در فیس‌بوک به اشتراک گذاشته شده بود.

از طریق این وب‌سایت‌ها، راپلر سرانجام موفق شد صاحب بالقوه‌ی این ۲۶ حساب کاربری را ردیابی کند: شخصی به نام رادن آلفارو پایاس.

ردیابی گردانندگان حساب‌های کاربری جعلی

مانند بسیاری از وب‌سایت‌هایی که راپلر فعالیتشان را زیر نظر دارد، سوابق ثبت دامنه‌ی OKD2.com هم خصوصی هستند. هیچ اطلاعاتی در خصوص نویسندگان و مالکان وب‌سایت بر روی آن موجود نیست و تنها راه تماس، استفاده از فرم تماس وب‌سایت است. خوشبختانه، ما توانستیم از سوابق دامنه برای شناسایی افراد مرتبط با وب‌سایت استفاده کنیم.

با استفاده از domaintools.com، متوجه شدیم که وب‌سایت OKD2.com از ژوئیه‌ی ۲۰۱۵ متعلق به فردی به نام رادن پایاس، ساکن شهر تاناوان در استان باتانگاس است. همچنین متوجه شدیم که شناسه‌ی کاربری OKD2.com در وب‌سایت گوگل اَدسِنس با سایر وب‌سایت‌های به اشتراک گذاشته شده توسط ۲۶ حساب کاربری جعلی یکی است. ما شناسه‌های ادسنس این سایت‌ها را با مشاهده‌ی کد منبع صفحات آن‌ها و از طریق جستجوی دنباله‌ای از اعداد که با حروف ca-pub- شروع می‌شوند شناسایی کردیم. به هر حساب گوگل ادسنس یک شناسه‌ی منحصربه‌فرد داده می‌شود که با ca-pub شروع می‌شود، و هر صفحه از سایتی که به آن حساب مرتبط است، این کد را روی آن خواهد داشت.

علاوه بر سوابق دامنه، متوجه شدیم که نام کاربری یکی از این ۲۶ حساب (Raden Alfaro Payas Unofficial) است.

موفق شدیم حساب کاربری دیگری را متعلق به این فرد با نام کاربری realradenpayas پیدا کنیم که با برخی از حساب‌های کاربری جعلی تعامل داشت.

به‌عنوان مثال، این حساب کاربری در مورد پست لوویمین کانسیو که جنایات حکومت نظامی کارلوس را انکار می‌کرد، اظهارنظر کرده بود. حساب «واقعی» پایاس می‌گوید که او در دوران حکومت نظامی در دبیرستان تحصیل می‌کرد و «هرگز نشنیده بود» کسی کشته یا شکنجه شود.

شروع به کار شارک‌تنک

این ۲۶ حساب جعلی و گستره‌ی نفوذ و فعالیت آن‌ها الهام‌بخش راپلر برای ایجاد پایگاه داده‌ی خود به نام شارک‌تنک و جمع‌آوری داده‌ها از گروه‌ها و صفحات عمومی فیس‌بوک به‌طور خودکار بود. از آگوست ۲۰۱۹، راپلر تقریبا ۴۰هزار صفحه را با میلیون‌ها دنبال‌کننده رصد کرده است. آنچه که به‌عنوان تحقیق در مورد مجموعه‌ای از حساب‌های مشکوک آغاز شد، تبدیل به مطالعه‌ی مداوم شبکه‌ای از هزاران حساب، گروه و صفحه‌ی جعلی و واقعی شد که به دروغ‌پراکنی و تبلیغات، تحریف و تضعیف دموکراسی یک ملت می‌پرداختند.

ا.ب. مطالعه‌ی موردی: چگونه توانستیم ثابت کنیم بزرگ‌ترین صفحه‌ی حامی کمپین «جان سیاه‌پوستان ارزشمند است» (Black Lives Matter) در فیس‌بوک جعلی است

نوشته‌ی: **دانی اُسالیوان**

دانی اُسالیوان خبرنگار سی‌ان‌ان است و موضوعاتی را پوشش می‌دهد که در محل تلاقی فناوری و سیاست جای می‌گیرند. او بخشی از تیم تجاری سی‌ان‌ان است و از نزدیک با واحد تحقیق سی‌ان‌ان برای ردیابی و شناسایی کمپین‌های اطلاعات نادرست در فضای مجازی که رأی‌دهندگان آمریکایی را هدف قرار می‌دهند، همکاری می‌کند.

در تابستان و پاییز ۲۰۱۷، و با کشف تدریجی جزئیات تلاش گسترده‌ی روسیه برای تأثیرگذاری بر رأی‌دهندگان آمریکایی از طریق رسانه‌های اجتماعی، مشخص شد که آمریکایی‌های آفریقایی‌تبار و جنبش «Black Lives Matter» (بی‌ال‌ام) از اهداف اصلی کمپین کرملین برای پاشیدن بذر نفاق بوده‌اند. من و همکارانم در سی‌ان‌ان ماه‌ها مشغول تهیه‌ی گزارش در مورد نقش روسیه در گردانندگی بعضی از بزرگ‌ترین حساب‌های کاربری مرتبط با بی‌ال‌ام در رسانه‌های اجتماعی بودیم. در حین گفتگو با فعالان این کمپین گاهی این سؤال از من پرسیده می‌شد: «می‌دانی چه کسی بزرگ‌ترین صفحه‌ی کمپین بی‌ال‌ام در فیس‌بوک را اداره می‌کند؟»

باورش دشوار است اما هیچ‌کس حتی برجسته‌ترین فعالان بی‌ال‌ام در کشور و سازمان‌دهندگان رویدادها- هم پاسخ این سؤال را نمی‌دانستند. طبیعتا برخی گمان می‌کردند این صفحه از روسیه اداره می‌شود. اما تحقیقات ما نشان داد فرد واقعی پشت این حساب

کاربری نه روس بود و نه آمریکایی صفحه توسط یک مرد سفیدپوست استرالیایی اداره می‌شد.

این صفحه که نام «Black Lives Matter» را برای خود انتخاب کرده بود، کاملا موجه به نظر می‌رسید. تا آوریل ۲۰۱۸ بیش از ۷۰۰هزار دنبال‌کننده داشت. مرتبا محتواهایی در ارتباط با نابرابری و خشونت پلیس به اشتراک می‌گذاشت، کمک‌های مالی جمع‌آوری می‌کرد و حتی یک فروشگاه آنلاین هم داشت که کالاهایی با شعار بی‌ال‌ام می‌فروخت.

اداره کردن صفحه‌ای با این اندازه و بزرگی کار غیرمعمولی نیست. بعضی فعالان ترجیح می‌دهند نام خود را در صفحه قرار ندهند تا باعث جلب‌توجه اوباش فضای مجازی نشوند و یا کنجکاوی مقامات را که به دنبال ساکت کردن اعتراضات هستند برنیانگیزند. در خارج از ایالات متحده، امکان اداره‌ی صفحات به صورت ناشناس برای فعالیت دیجیتال فعالان بسیار مهم بوده و در برخی از جنبش‌ها عامل کلیدی بود. (این دقیقا همان چیزی بود که روسیه از آن سود جست و شک و تردیدها درباره‌ی ارتباط بی‌ال‌ام با روسیه نیز از همینجا ناشی می‌شد).

همان زمانی که توجه من به این صفحه‌ی مرموز جلب شده بود، جرمی ماسلر، یک محقق مستقل و از بهترین کارآگاه‌های فضای مجازی با یک سرنخ به سراغم آمد. ماسلر سوابق دامنه‌ی وب‌سایت‌هایی را که صفحه‌ی بزرگ بی‌ال‌ام مرتب به آن‌ها لینک می‌داد بررسی کرده بود.

اگرچه دامنه‌ها به‌صورت خصوصی ثبت شده بودند، او متوجه شده بود که یکی از آن‌ها در سال ۲۰۱۶ برای مدتی به فردی در پرث استرالیا تعلق داشته است؛ مردی سفیدپوست به نام ایان مک‌کی.

```
Domain Name: BLACKLIVESMATTERWEBSITE.COM
Registry Domain ID: 2065833077_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.launchpad.com
Registrar URL: LaunchPad.com
Updated Date: 2018-10-13T08:00:42Z
Creation Date: 2016-10-13T07:10:33Z
Registrar Registration Expiration Date: 2018-10-13T07:10:33Z
Registrar: Launchpad, Inc. (HostGator)
Registrar IANA ID: 955
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Not Available From Registry
Registrant Name: ian mackay
Registrant Organization: Website
Registrant Street: [redacted]
Registrant City: brisbane
Registrant State/Province: Queensland
Registrant [redacted]
Registrant
Registrant
Registrant
Registrant
Registrant Fax Ext:
Registrant Email: blacklivesmatter1@hotmail.com
```

ماسلر با مک‌کی تماس گرفت و او مدعی شد برای سرگرمی به خرید و فروش دامنه می‌پردازد و هرگونه ارتباطی با صفحه‌ی فیس‌بوک بی‌ال‌ام را انکار کرد. چند ماه بعد، زمانی که من با مک‌کی، از مقامات میان‌سال اتحادیه‌ی کارگران استرالیا، تماس گرفتم پاسخ مشابهی به من داد. اما آن زمان متوجه شدیم که مک‌کی ده‌ها نام وب‌سایت را ثبت کرده که بسیاری از آنها به فعالیت‌های سیاهپوستان مربوط می‌شدند.

علی‌رغم نگرانی‌هایم در مورد این صفحه و این واقعیت که چند فعال به من گفته بودند به آن مشکوک هستند، توضیح مک‌کی در ظاهر غیرقابل‌باور نبود. نام‌های دامنه می‌توانند ارزشمند باشند و مردم همیشه آن‌ها را خرید و فروش می‌کنند. این واقعیت که او همچنین دامنه‌هایی را که مرتبط با فعالیت‌های سیاهپوستان نبود ثبت کرده و فروخته بود، ادعایش را بیش از پیش معتبر جلوه می‌داد. اما بعد اتفاق عجیبی افتاد. چند دقیقه بعد از صحبت من با مک‌کی، صفحه‌ی بی‌ال‌ام در فیس‌بوک از کار افتاد. فیس‌بوک آن را حذف نکرده بود، بلکه توسط هر کسی که آن را اداره می‌کرد موقتا از دسترس خارج شده بود.

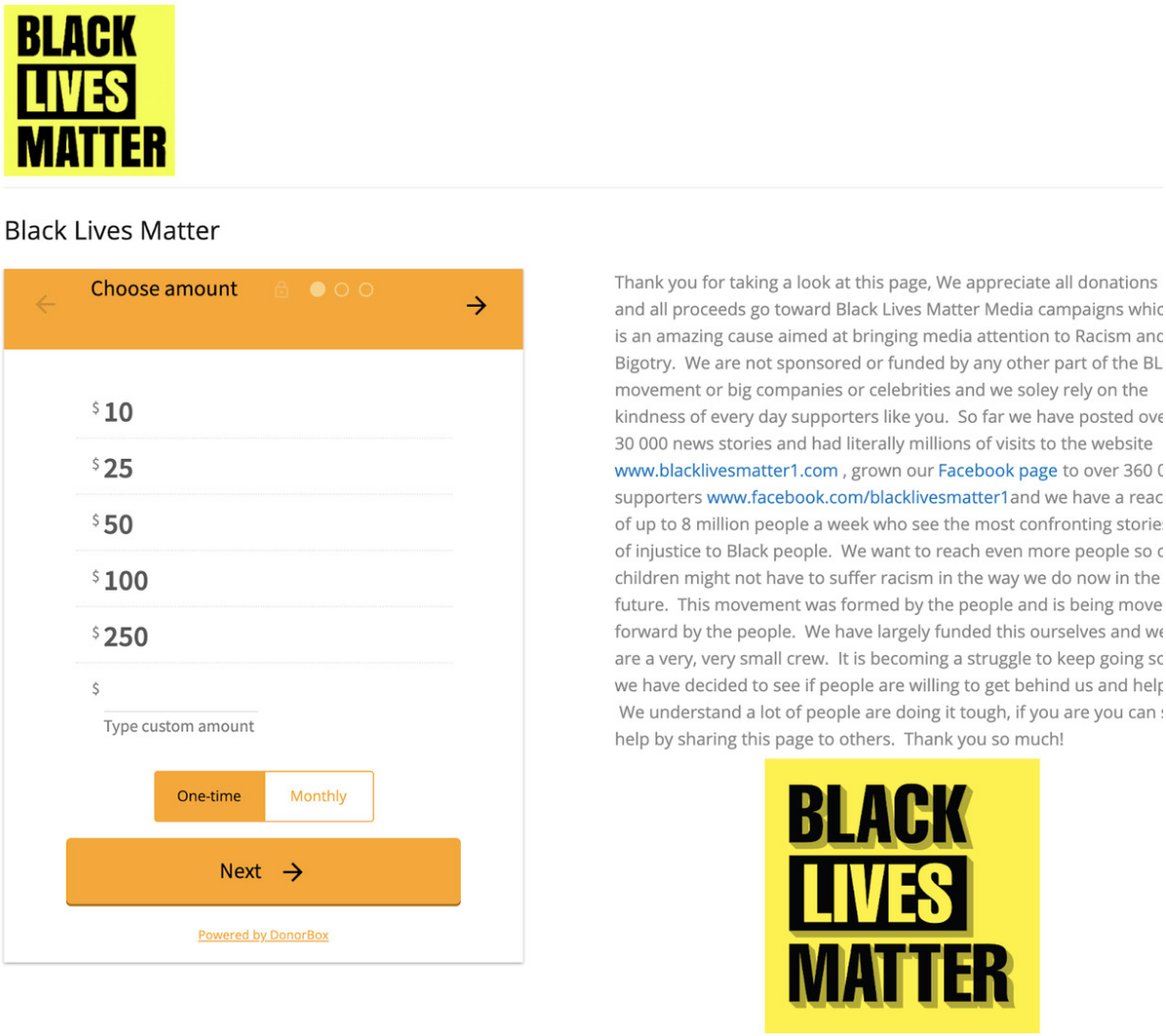
این مسئله کاملا مشکوک بود و باعث شد من و ماسلر تصمیم بگیریم بیشتر درباره‌اش کنکاش کنیم.

صفحه‌ی فیس‌بوک که چند هفته پس از تماس من با مک‌کی دوباره آنلاین شد، در طول فعالیت‌هایش کمپین‌های جمع‌آوری کمک‌های مالی را که ظاهرا برای حمایت از بی‌ال‌ام برپا شده بودند، تبلیغ کرده بود.

در یک نمونه از این تبلیغات ادعا شده بود کمپین جهت جمع‌آوری کمک‌های مالی برای فعالان در ممفیس، تنسی برگزار شده است. اما وقتی با فعالان آنجا صحبت کردم، هیچ‌کس چیزی در مورد جمع‌آوری کمک مالی یا اینکه ممکن است این پول کجا رفته باشد، نمی‌دانست. فعالان دیگر حتی به ما گفتند که به گمان اینکه این یک کلاهبرداری است، صفحه را به فیس‌بوک گزارش کرده‌اند اما شرکت هیچ اقدامی نکرده بود.

هنگامی که شروع به تماس با پلتفرم‌های پرداخت آنلاین و جمع‌آوری کمک‌های مالی متعددی کردم که صفحه از آن استفاده می‌کرد، آن شرکت‌ها شروع به حذف این کمپین‌های جمع‌آوری کمک کردند و گفتند که این کمپین‌ها قوانین آن‌ها را زیر پا گذاشته‌اند. با استناد به قوانین مربوط به حفظ حریم

خصوصی کاربر، هیچ‌یک از شرکت‌های پرداخت آنلاین حاضر نشدند اطلاعاتی در مورد اینکه پول کجا رفته است به من ارائه کنند. این یک چالش رایج است. با استناد به سیاست‌های حفظ حریم خصوصی، پلتفرم‌ها و خدمات دیجیتالی به‌ندرت نام یا اطلاعات تماس دارندگان حساب را در اختیار مطبوعات قرار می‌دهند.



بعدتر، از طریق فردی که با بعضی از این پرداخت‌های صورت گرفته آشنایی داشت، فهمیدم که حداقل

یکی از این پرداخت‌ها از طریق یک بانک و آدرس آی‌پی استرالیایی صورت گرفته است. منبع دیگری به من گفت که حدود ۱۰۰هزار دلار کمک نقدی جمع‌آوری شده است. پیدا کردن منابعی در شرکت‌های فناوری که مایل باشند اطلاعاتی در اختیارتان قرار بدهند که شرکت از ارائه‌ی آن‌ها خودداری می‌کند اهمیت فزاینده‌ای پیدا کرده است، چراکه به دلیل پیشرفته‌تر شدن ترفندهای کلاهبرداران و عاملان بد، بسیاری از داستان‌ها را نمی‌توان صرفا با استفاده از داده‌های منبع‌باز کشف کرد.

اطلاعاتی را که به دست آورده بودم در اختیار فیس‌بوک قرار دادم و از آن‌ها خواستم در مورد این داستان نظر بدهند. گفتم شواهدی دارم که نشان می‌دهد صفحه به استرالیا مرتبط است، شرکت‌های پرداخت آنلاین پس از بررسی، کمپین‌ها را حذف کرده‌اند و ما می‌دانیم که بخشی از پول به استرالیا می‌رود. یکی از سخنگویان فیس‌بوک گفت که تحقیقات این پلتفرم رسانه‌ی اجتماعی «هیچ نشانه‌ای از اینکه قوانین و استانداردهای این پلتفرم نقض شده باشد، پیدا نکرده است».

اندکی قبل از انتشار گزارش ما - و تنها پس از اینکه من نگرانی خود در مورد تحقیقات فیس‌بوک و پاسخ سخنگوی آن را با یکی از کارمندان ارشد فیس‌بوک مطرح کردم - بود که فیس‌بوک بالاخره اقدام به حذف صفحه کرد.

پس از گزارش سی‌ان‌ان، اتحادیه‌ی کارگران استرالیا که مک‌کی در آن کار می‌کرد، تحقیقات خود را آغاز کرد. در پایان هفته، مک‌کی و یک مقام دیگر اتحادیه که او نیز در این کلاهبرداری دخیل بود اخراج شدند.

نکته‌ی قابل‌توجه در این داستان طیف گسترده‌ی تکنیک‌هایی بود که ماسلر و من برای رسیدن به نتیجه استفاده کردیم. ما به‌شدت به سایت‌های بایگانی مانند Wayback Machine متکی بودیم که به ما این امکان را می‌داد که ظاهر وب‌سایت‌هایی را که صفحه به آن‌ها پیوند داشت و همچنین خود صفحه را قبل از اینکه توجه ما به آن معطوف شود، ببینیم. این کار به‌ویژه از این لحاظ اهمیت داشت که پس از تماس ماسلر با مک‌کی، اداره‌کنندگان سایت شروع به تلاش برای پنهان کردن ردپای خود کردند.

ما همچنین از خدماتی که ثبت دامنه را ردیابی می‌کنند، از جمله DomainTools.com، برای بررسی سایت‌هایی که مک‌کی ثبت کرده بود و همچنین برای پیدا کردن اطلاعات تماس او استفاده کردیم.

ماسلر همچنین از Facebook Graph Search (ابزاری که دیگر موجود نیست) برای شناسایی حساب‌های جعلی‌ای که جهت تبلیغ این صفحه در فیس‌بوک ایجاد شده بودند، استفاده‌ی فراوان کرد. بررسی اطلاعات منبع‌باز و استفاده از ابزارهای تحقیقاتی آنلاین، مانند ابزارهایی که برای دسترسی به سوابق دامنه استفاده می‌شوند، حیاتی هستند اما تنها استفاده از ابزارها کافی نیست.

اقدام ساده‌ی برداشتن گوشی تلفن و تماس با مک‌کی و پیدا کردن منابعی برای دسترسی به اطلاعاتی که عمومی نیستند و در حالت عادی نمی‌توان به آن‌ها دسترسی پیدا کرد -یعنی تکنیک‌های سنتی روزنامه‌نگاری- در افشای این کلاهبرداری بسیار مهم بود.

۲. پیدا کردن بیمار صفر

نوشته‌ی: **هنک فن اِس**

هنک فن‌اِس مشاور شبکه‌ی بین‌المللی فکت‌چکینگ پوینتر است. او علاقه‌ی وسواس‌گونه‌ای به پیدا کردن داستان‌های نهته در داده‌ها دارد. فن‌اس متخصصان رسانه در سراسر جهان را در زمینه‌ی تحقیقات اینترنتی، رسانه‌های اجتماعی و چندرسانه‌ای آموزش می‌دهد. مشتریان او عبارتند از ان‌بی‌سی نیوز، بازفید نیوز، آی‌تی‌وی، گلوبال ویتنس، اس‌آراف، آکسل اسپرینگر و بسیاری سازمان‌های غیرانتفاعی و دانشگاه‌ها. وب‌سایت‌های او، whopostedwhat.com و graph.tips، برای جستجوی اطلاعات خاص در شبکه‌های اجتماعی کاربرد فراوان دارند. او با نام کاربری @henkvaness در توئیتر فعالیت می‌کند.

مهمان‌دار هواپیما، گائتان دوگاس کانادایی، تا دهه‌ها به‌عنوان بیمار صفر شناخته می‌شد؛ اولین فرد مبتلایی که بیماری ایدز را به ایالات متحده آورد. این ویژگی که از طریق فیلم‌ها، کتاب‌ها و گزارش‌های بی‌شمار به آن پرداخته و تقویت می‌شد، از گائتان چهره‌ی یک فرد شریر را ساخته بود؛ شریری که آغازکننده‌ی پاندمی‌ای بود که درنهایت منجر به مرگ بیش از ۷۰۰هزار نفر در آمریکای شمالی شد.

اما قضیه درواقع این نبود. بیل دَرو، بازرس مرکز کنترل و پیشگیری از بیماری‌ها، با دوگاس مصاحبه کرده و اطلاعات او را تحت عنوان بیمار O (اُ) در فایل‌ها ثبت کرده بود.

اُ مخفف Out of California (خارج از کالیفرنیا) بود. اما به‌زودی حرف O با عدد 0 اشتباه گرفته شد؛ اشتباهی که باعث ایجاد زنجیره‌ای از اطلاعات نادرست شد که تا همین اواخر هم ادامه داشت.

این خطر برای روزنامه‌نگاران نیز وجود دارد که در صورت به خرج ندادن دقت کافی، توجه خود را معطوف به یک بیمار صفر اشتباه کنند. این فصل به شما کمک می‌کند با خلاص شدن از دست اطلاعات سطحی و جستجوی عمیق‌تر، منابع دست‌اول در فضای مجازی را شناسایی کنید.

۱.خطرات استفاده از منابع دست‌اول و چگونگی فائق آمدن بر آن‌ها

روزنامه‌نگاران عاشق منابع دست‌اول در فضای مجازی هستند. شواهد دست‌اول ممکن است در یک مقاله‌ی روزنامه، یک مطالعه‌ی علمی، یک بیانیه‌ی مطبوعاتی، شبکه‌های اجتماعی و یا در هر «بیمار صفر» احتمالی دیگری یافت شوند.

جستجوی ساده‌ی یک واژه‌ی کلیدی در وب‌سایت یک سازمان دولتی ممکن است این تصور را برایتان ایجاد کند که نتایجی که می‌بینید همه‌ی آن‌چیزی است که آن‌ها در خصوص موضوع مورد نظر در اختیار دارند؛ تصوری که در غالب موارد اشتباه است. برای مثال اجازه بدهید به سراغ وب‌سایت کمیسیون بورس و اوراق بهادار آمریکا برویم؛ منبعی که برای پیدا کردن اطلاعات مالی در خصوص شهروندان ایالات متحده و تجار سراسر دنیا به کار برده می‌شود. تصور کنید هدف پیدا کردن اولین مورد استفاده از عبارت «پلیس هلندی (Dutch police)» در وب‌سایت کمیسیون بورس و اوراق بهادار (sec.gov) باشد. موتور جستجوی داخلی سایت sec.gov می‌تواند برای این کار کمکمان کند:

نتیجه تنها شامل یک سند مربوط به سال ۲۰۱۶ است. بنابراین، کمیسیون در سال ۲۰۱۶ فقط یک بار از این اصطلاح استفاده کرده است؛ درست است؟

> And I have cooperated with the FBI in the pump and dump scam. The Dutch police. The same thing, with the Scotland Yard over the years. And I certainly understand fraud and fraudulent activities.

خیر. این اصطلاح اولین بار ۱۲ سال پیش از آن و در سال ۲۰۰۴ در یک ایمیل رمزگذاری‌شده‌ی محرمانه در sec.gov به کار برده شده است:

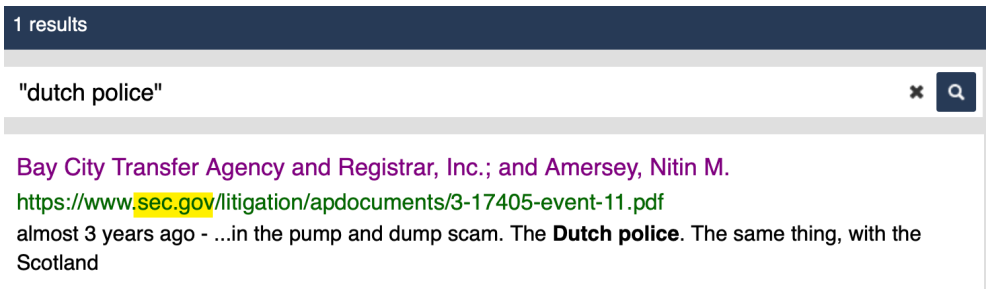
```
The increase was
primarily the result of several large international contract
awards, such as the Dutch Police, an Australian utilities
company and a Russian utilities company, and additional orders
received for Z/I Imaging Digital Mapping Cameras.
```

اگرچه این نتیجه مستقیما از وب‌سایت sec.gov به دست آمده است، اما با وارد کردن واژه‌ی کلیدی مورد نظر در موتور جستجوی سایت آن را پیدا نخواهید کرد. این تفاوت به چه دلیل است؟ شما باید به‌صورت پیش‌فرض همیشه نسبت به موتورهای جستجوی منابع دست‌اول بی‌اعتماد باشید. آن‌ها می‌توانند تصور نادرستی از محتوای واقعی وب‌سایت و پایگاه‌های داده‌ی مرتبط با آن به شما بدهند. راه مناسب برای جستجو انجام «بررسی منبع اولیه» است.

بررسی منابع اولیه

قدم اول: به لینک ناقص دقت کنید.

نتیجه‌ی جستجو در وب‌سایت sec.gov تنها یک مورد را در اختیار ما قرار داد:

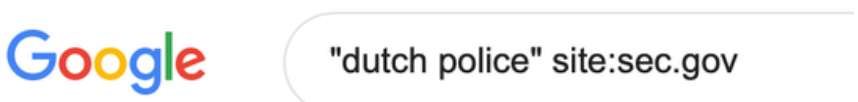


بیایید با همین نتیجه‌ی مأیوس‌کننده شروع کنیم. ابتدا قسمت اول لینک، یعنی https://www، را حذف کنید. حواستان به اولین بک‌اسلش (/) باشد که در این مثال قبل از واژه‌ی "/litigation" قرار گرفته است.

بخشی که ما نیاز داریم این است: sec.gov

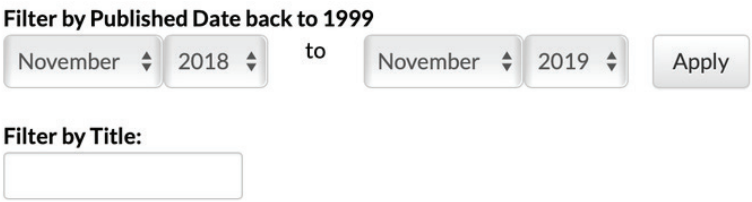
گام دوم: استفاده از واژه‌ی site:

به هر موتور جستجویی که ترجیح می‌دهید بروید. اول واژه‌ی کلیدی مورد نظرتان ("Dutch police") را وارد کنید و در آخر هم اضافه کنید "site:" و به دنبال آن بدون فاصله URL موردنظر را وارد کنید. از این راه می‌توانید مطمئن شوید آیا منبع اولیه‌ی موردنظر همه‌ی اطلاعات موجود را به شما نشان داده است یا نه:



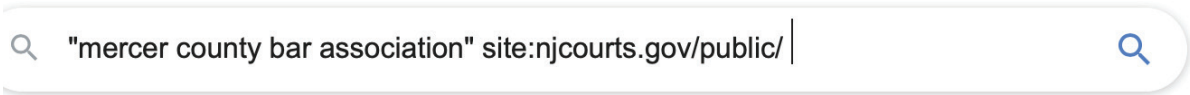
گنجاندن پوشه‌های خاص در جستجو

اکنون می‌توانید این فرمول جستجو در منبع اصلی را بر حسب نیازهای خود تغییر بدهید. اجازه بدهید به بخش بیانیه‌های مطبوعاتی وب‌سایت دادگاه‌ی نیوجرسی برویم. تصور کنید می‌خواهید به دنبال خبر حمایت کانون وکلای مرسر کانتی از برنامه‌ی روز حقوق قضایی بگردید، اما نمی‌توانید منبع اولیه را در عنوان هیچکدام از بیانیه‌های مطبوعاتی پیدا کنید. «کانون وکلای مرسر کانتی» در هیچ عنوانی دیده نمی‌شود.



حالا به URL این صفحه نگاه کنید که پر است از بیانیه‌های مطبوعاتی‌ای که به روشی ناکارآمد ذخیره و فهرست شده‌اند:

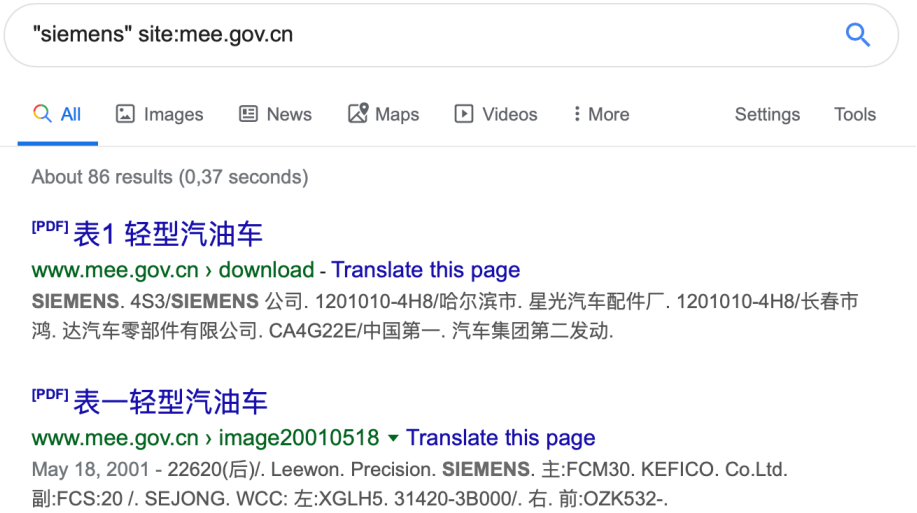
مطالب مربوط به روابط عمومی در پوشه‌ی public آرشیو شده‌اند. باید در جستجوی گوگل خود این نکته را بگنجانید:



و این هم نتیجه:

پیش‌بینی پوشه‌ها

چین یک وزارت بوم‌شناسی و محیط زیست دارد. آیا آن‌ها مدارکی به زبان انگلیسی در مورد شرکت آلمانی زیمنس دارند؟ با فرمول زیر، اسناد به زبان‌های چینی و انگلیسی را در نتایج جستجو دریافت خواهید کرد:



حالا فرض کنید می‌خواهید جستجوی خود را باز هم فیلتر کنید تا فقط نتایج انگلیسی را ببینید. شاید آن‌ها از کلمه‌ی انگلیسی در لینک استفاده کرده باشند؟ امتحانش کنید. جواب می‌دهد:

۲. دنبال کردن رد اسناد

گاهی اوقات اطلاعات مورد نیاز ما در خود صفحه‌ی وب موجود نیست، بلکه درواقع در سندی است که توسط وب‌سایت میزبانی شده است. در اینجا نحوه‌ی دنبال کردن رد سند با استفاده از فرمول‌های گوگل آورده شده است.

راس مک‌کیتریک دانشیار گروه اقتصاد در دانشگاه گوئلف انتاریو است. در سال ۲۰۱۴، او سخنرانی‌ای برای گروهی از شکاکان به صحت ادعای تغییرات آب‌وهوایی ارائه داد. بیایید سعی کنیم دعوتنامه‌ی آن جلسه را پیدا کنیم. می‌دانیم که سخنرانی در۱۳ مه ۲۰۱۴ برگزار شده است و یازدهمین رویداد سالانه‌ی بنیان دوستان علم (FSO) بوده است. اگر این عبارات را در گوگل جستجو کنیم، هیچ نتیجه‌ای نشان داده نخواهد شد:

No results found for **"Friends of Science 11th Annual Luncheon 2014" "invitation"**.

چرا؟ چون اصولا کلمه‌ی دعوتنامه در بسیاری از دعوت‌نامه‌ها ذکر نمی‌شود. در خصوص کلمه‌ی مصاحبه هم همینطور است. بسیاری از مصاحبه‌ها حاوی کلمه‌ی مصاحبه نیستند. حتی در بیشتر نقشه‌ها نیز کلمه‌ی نقشه به‌صراحت روی آن‌ها نوشته نشده است. توصیه‌ی من؟ دست از حدس زدن بردارید، آرامش خود را حفظ کنید و به شهود درونی‌تان اطمینان کنید.

مرحله‌ی اول: مشخص کردن نوع مدرک

سعی کنید وجه اشتراک تمام دعوتنامه‌های آنلاین را پیدا کنید. دعوتنامه‌ها معمولا در قالب یک فایل پی‌دی‌اف هستند. این احتمال را با افزودن "filetype:pdf" به جستجوی خود بیازمایید. شاید موفق شوید دعوتنامه‌ی مورد نظر را پیدا کنید.

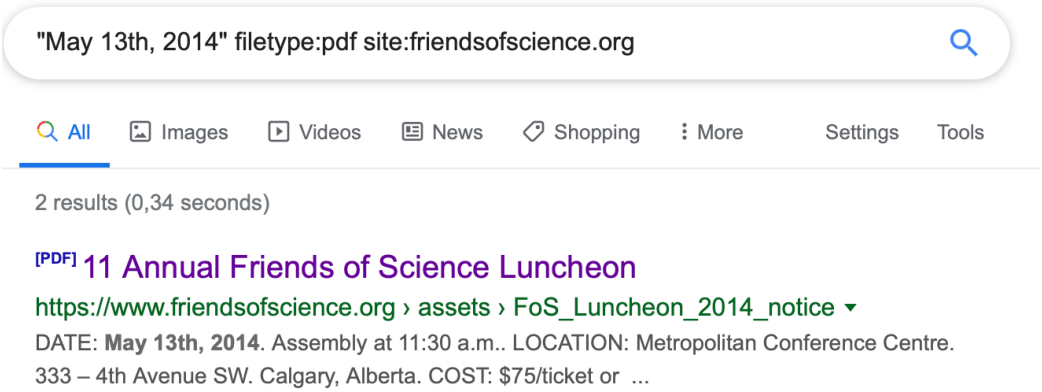
مرحله‌ی دوم: بی‌طرف باشید

درست است که از کلماتی که در متن دعوتنامه آمده اطلاع ندارید، اما می‌دانید ویدئوی یوتیوب مربوط به رویدادی است که در ۱۳ مه ۲۰۱۴ برگزار شده بوده است. ممکن است این تاریخ در متن دعوتنامه درج شده باشد (مطمئن شوید هم اعداد وضعی و هم اعداد ترتیبی را در جستجوی خود وارد می‌کنید، یعنی May 13 و May 13th)

مرحله‌ی سوم: چه کسانی با این رویداد مرتبط هستند

ما می‌دانیم که برگزارکننده‌ی این رویداد سازمان دوستان علم بوده و وب‌سایت آن‌ها friendsofscience.org است.

وقتی هر سه‌ی این مراحل را با هم ادغام می‌کنید، نتایج جستجوی شما در گوگل به این شکل خواهد بود:



گزینه‌ی اول نتایج همان چیزی است که به دنبالش بودید: دعوتنامه‌ی سخنرانی.

دوستان علم، مستقر در شهر کلگری، اغلب به عنوان یک گروه انکار تغییرات آب‌وهوایی شناخته می‌شود و تا حدی توسط بخش نفت و گاز تأمین مالی می‌شود. سؤال این است که چگونه می‌توانیم یک جستجوی کارآمد برای یافتن اطلاعات بیشتر در مورد این گروه و شبکه‌ی حامیان و تأمین‌کنندگانش داشته باشیم؟

مرحله‌ی اول: هدف را در جستجوی خود بگنجانید

جستجوی واژه‌ی کلیدی دوستان علم به‌تنهایی نتایج بسیار زیادی به دست خواهد داد؛ بنابراین بهتر است شهر محل استقرار سازمان را نیز در جستجوی خود بگنجانید: کلگری

مرحله‌ی دوم: "filetype:" را در جستجوی خود بگنجانید

بهترین گزینه‌ای را که برای تمام اسناد رسمی به ذهنتان می‌رسد امتحان کنید: "filetype:pdf".

مرحله‌ی سوم: وب‌سایت هدف خود را حذف کنید

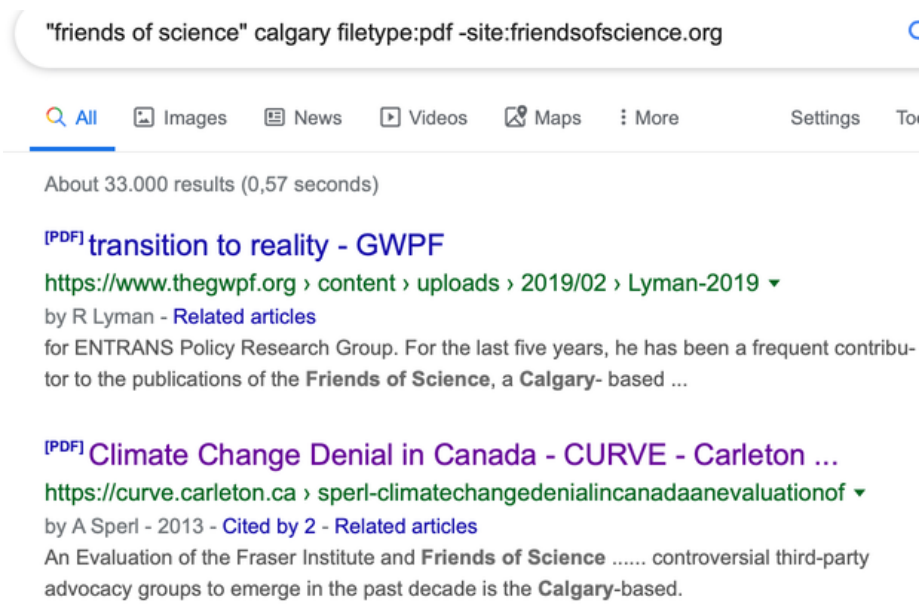
با افزودن "-site:friendsofscience.org"، وب‌سایت هدف Friendsofscience.org را حذف کنید.

این کمکتان خواهد کرد فقط نتایج مربوط به منابع خارج از سازمان را مشاهده کنید.

عبارت کامل شما برای جستجو به این شکل خواهد بود:

```
"friends of science" calgary filetype:pdf -site:friendsofscience.org
```

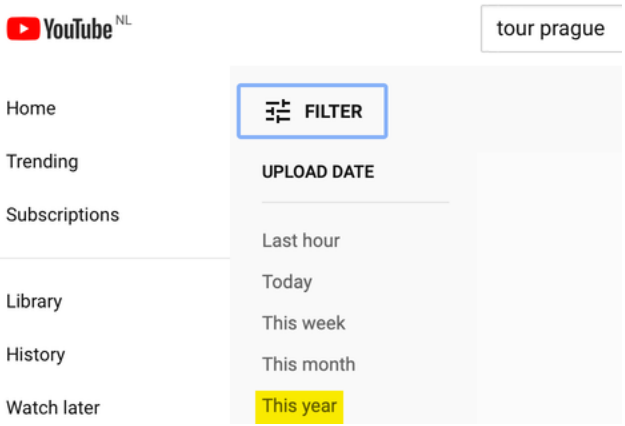
از آنجایی که هدف را در اسناد رسمی‌ای جستجو کرده‌اید که روی وب‌سایت خود سازمان قرار ندارند، احتمالا نتایج شامل برخی هم‌رزمان و طرفداران و درعین‌حال برخی از منتقدان سازمان خواهد بود:



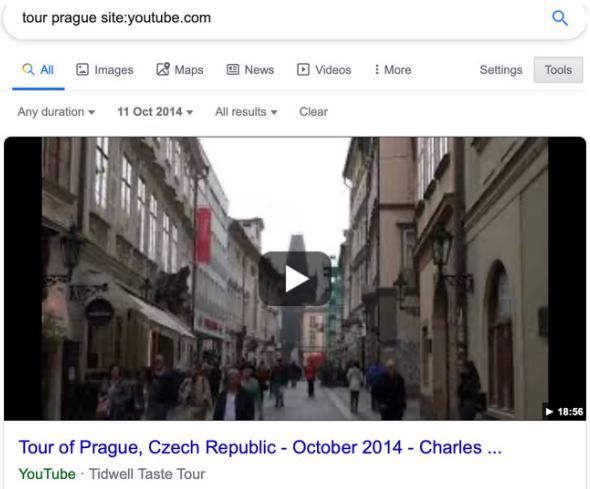
۳. غربال کردن رسانه‌های اجتماعی برای منابع اولیه

یوتیوب

ابزار جستجوی یوتیوب یک مشکل دارد: به شما امکان غربال کردن ویدئوهای قدیمی‌تر از یک سال را نمی‌دهد. اگر بخواهید ویدئویی از تور گردشگری پراگ از ۱۱ اکتبر ۲۰۱۴ را تماشا کنید، این مانعی است که با آن مواجه خواهید شد:



برای حل این مشکل، با استفاده از منوی Tools در منتهی‌الیه دست راست بالای صفحه، تاریخ مورد نظر خود را به‌صورت دستی در google.com وارد کنید. سپس گزاره‌های "Any time" و "Custom Range" را انتخاب کنید. به‌این‌ترتیب، نتایج مورد نیاز خود را به دست خواهید آورد:

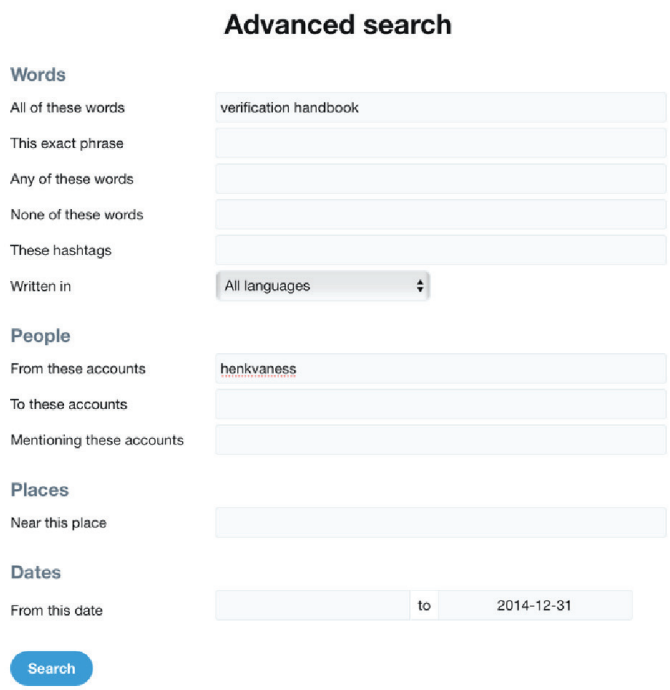


توئیتر

با وجود قدرت و کارآیی اپراتور جستجوی "site:"، اگر از آن در گوگل برای جستجو در توئیتر استفاده کنید، ناامید خواهید شد. به‌عنوان مثال، اجازه بدهید برای جستجوی اولین باری که درباره‌ی کتابچه‌ی راهنمای راستی‌آزمایی توئیت کردم، این عبارت را امتحان کنیم:

"verification handbook" site:twitter.com/henkvaness

تا زمان حاضر که مشغول نوشتن این مقاله هستم، نتیجه‌ی این جستجو تنها شامل یک گزینه است. موتورهای جستجوی عمومی مانند گوگل اغلب برای استخراج نتایج با کیفیت از میلیاردها پست در توئیتر یا پلتفرم‌های بزرگ دیگر مانند فیس‌بوک و اینستاگرام کارآیی چندانی ندارند. به‌جای آن می‌توان از قابلیت جستجوی پیشرفته‌ی توئیتر استفاده کرد؛ کلمات کلیدی، بازه‌های زمانی و نام کاربری مورد نظرتان را به این شکل وارد کنید:



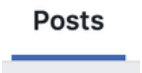
فراموش نکنید روی گزینه‌ی "Latest" در منوی بالای صفحه‌ی نتایج جستجو کلیک کنید تا بتوانید نتایج را به ترتیب زمانی معکوس مشاهده کنید. در غیر این صورت توئیتر به‌طور پیش‌فرض نتایج شما را بر اساس توئیت‌های برتر مرتب می‌کند.

فیس‌بوک

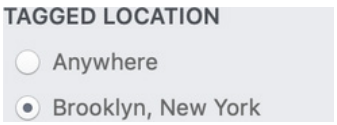
در این شبکه‌ی اجتماعی نیز استفاده از "site:" کمک چندانی نمی‌کند، اما می‌توانیم جستجوگر خود وب‌سایت را به‌گونه‌ای تنظیم کنیم که پاسخگوی نیازهایمان باشد. به‌عنوان مثال، تصور کنید می‌خواهید تمام پست‌هایی را که در سال ۲۰۱۹ درباره‌ی کیک توت‌فرنگی توسط مردم بروکلین به اشتراک گذاشته شده ببینید. این مراحل را دنبال کنید:

قدم اول: عبارت مورد نظر خود را در جستجوگر وارد کنید:

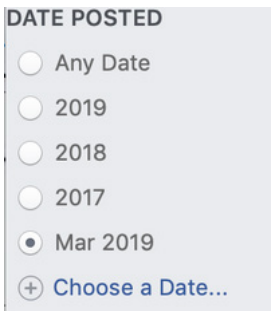
قدم دوم: روی گزینه‌ی Posts کلیک کنید



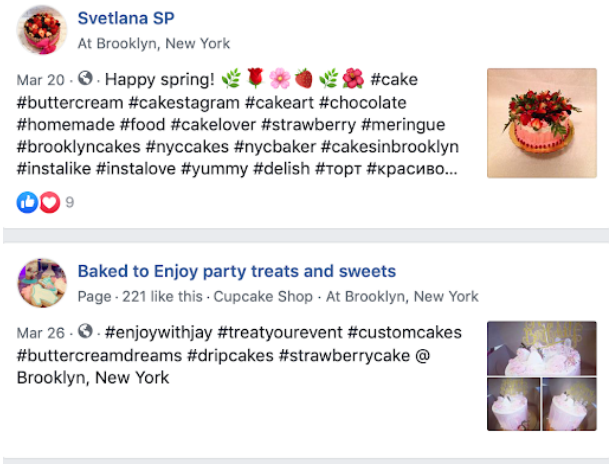
قدم سوم: موقعیت مکانی خود را مشخص کنید



قدم چهارم: یک تاریخ انتخاب کنید

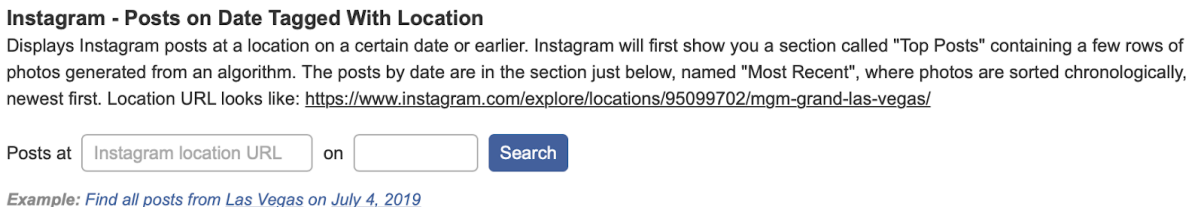


و این هم نتیجه‌ی جستجو:



اینستاگرام

برای جستجوی پست‌های اینستاگرام در یک تاریخ و محل خاص می‌توانید به وب‌سایت من، whopostedwhat.com، بروید و فرم جستجو را پر کنید:



۳. شناسایی ربات‌ها، سایبورگ‌ها و فعالیت‌های غیرواقعی

نوشته‌ی: **یوهانا وایلد و شارلوت گدار**

شارلوت گدار محقق و مدرس بِلینگ‌کَت است. او پیش از انتقال به بلینگ‌کت در مرکز حقوق بشر دانشگاه برکلی، کالیفرنیا فعالیت می‌کرد. وی در برکلی در آزمایشگاه تحقیقاتی کار می‌کرد و درعین‌حال وظیفه‌ی آموزش دانشجویان برای انجام تحقیقات با استفاده از داده‌های منبع‌باز در مورد درگیری‌های جهانی برای نهادهای بشردوستانه‌ی بین‌المللی را نیز بر عهده داشت.

یوهانا وایلد محقق داده‌های منبع‌باز در بلینگ‌کت است. او همچنین بر توسعه‌ی فناوری و ابزار برای تحقیقات دیجیتال نیز تمرکز دارد. او سابقه‌ی روزنامه‌نگاری آنلاین را نیز دارد و پیش از این در مناطق (پسا)درگیری با روزنامه‌نگاران کار کرده است. یکی از نقش‌های او حمایت از روزنامه‌نگاران در شرق آفریقا برای تولید برنامه جهت پخش در صدای آمریکا بود.

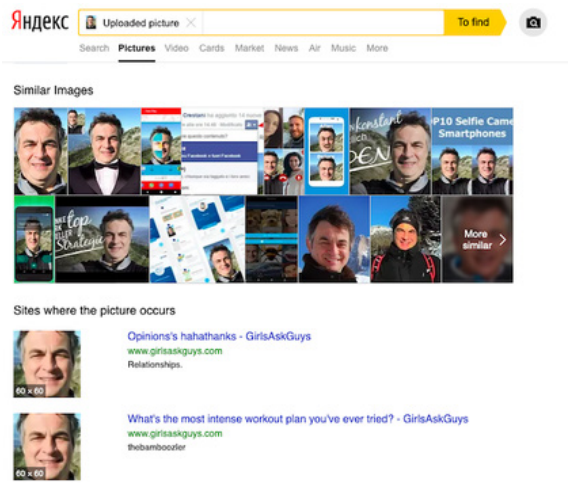
اواخر آگوست ۲۰۱۹، بنجامین استریک، نویسنده‌ی بلینگ‌کت و محقق بی‌بی‌سی آفریقا آی حین تحلیل توئیت‌هایی که هشتگ‌های #WestPapua و #FreeWestPapua را منتشر می‌کردند متوجه وجود بعضی حساب‌های کاربری شد که الگوی فعالیت غیرعادی‌ای داشتند. این حساب‌های کاربری همگی پیام‌هایی در طرفداری از دولت اندونزی منتشر می‌کردند و این در حالی بود که توجه جامعه‌ی بین‌المللی اندک‌اندک به درگیری‌ها در پاپوآی غربی جلب می‌شد؛ یک جنبش استقلال محلی برای مطالبه‌ی آزادی از سلطه‌ی اندونزی به خیابان‌ها آمده بودند و درگیری‌ها بین تظاهرکنندگان و پلیس اندونزی به خشونت کشیده شده بود.

حساب‌های کاربری‌ای که توجه استریک را جلب کرده بودند شباهت‌های عجیب متعددی با هم داشتند. او به زودی متوجه شد که این شباهت‌ها نشانه‌های اولیه‌ی فعالیت‌های غیرواقعی هماهنگ‌شده هستند. اما در ابتدا همین نکات کوچک بود که توجه او را جلب کرد.

به‌عنوان مثال، بسیاری از حساب‌ها از عکس‌های جعلی و دزدیده‌شده استفاده کرده بودند.

حساب کاربری زیر را در نظر بگیرید که ادعا می‌کند متعلق به شخصی به نام مارکو است:

استریک با استفاده از ابزار جستجوی معکوس عکس Yandex متوجه شد که این عکس پیش از آن در وب‌سایت‌های دیگر با نام‌های مختلف استفاده شده است. هیچ‌کدام از حساب‌هایی که از این عکس استفاده کرده بودند متعلق به شخصی واقعی به نام «مارکو» نبودند. این ثابت می‌کرد که این حساب‌های کاربری دست‌کم قصد گمراه کردن کاربران درباره‌ی هویت واقعی خود را دارند.



علاوه بر جعل هویت، استریک همچنین متوجه شد که حساب‌ها محتواهای مشابه یا حتی یکسانی را

منتشر کرده‌اند و اغلب یکدیگر را ریتوییت می‌کنند. حتی جالب‌تر این بود که برخی از آن‌ها هماهنگی دقیقی در الگوهای کد زمانی توئیت‌هاشان نشان دادند.

به عنوان مثال، @bellanow1 و @kevinma40204275 بیشتر توئیت‌های خود را در دقیقه‌ی ۷ یا دقیقه‌ی ۳۲ هر ساعت خاص منتشر می‌کردند.

26/8/19	17:07:37	bellanow1	26/8/19	23:07:20	kevinma40204275
26/8/19	5:27:06	bellanow1	26/8/19	21:32:52	kevinma40204275
26/8/19	5:27:06	bellanow1	26/8/19	20:32:52	kevinma40204275
26/8/19	5:27:05	bellanow1	26/8/19	18:32:51	kevinma40204275
26/8/19	5:27:04	bellanow1	26/8/19	15:07:22	kevinma40204275
26/8/19	5:27:04	bellanow1	26/8/19	12:32:54	kevinma40204275
26/8/19	3:32:55	bellanow1	26/8/19	9:32:54	kevinma40204275
26/8/19	0:32:56	bellanow1	26/8/19	5:32:54	kevinma40204275
26/8/19	0:07:33	bellanow1	26/8/19	5:07:36	kevinma40204275
25/8/19	23:32:54	bellanow1	26/8/19	3:32:54	kevinma40204275
25/8/19	22:32:53	bellanow1	26/8/19	0:32:54	kevinma40204275
25/8/19	22:07:06	bellanow1	25/8/19	23:32:52	kevinma40204275
25/8/19	20:32:53	bellanow1	25/8/19	23:07:16	kevinma40204275
25/8/19	10:07:19	bellanow1	25/8/19	19:32:53	kevinma40204275
25/8/19	9:32:56	bellanow1	25/8/19	15:07:24	kevinma40204275
25/8/19	9:07:27	bellanow1	25/8/19	10:32:55	kevinma40204275
25/8/19	8:32:56	bellanow1	25/8/19	7:32:55	kevinma40204275
25/8/19	7:07:23	bellanow1	25/8/19	6:32:54	kevinma40204275
25/8/19	6:32:56	bellanow1	25/8/19	6:08:01	kevinma40204275
24/8/19	13:07:57	bellanow1	25/8/19	3:07:21	kevinma40204275
24/8/19	10:07:19	bellanow1	25/8/19	0:07:26	kevinma40204275
24/8/19	7:32:56	bellanow1	24/8/19	20:32:51	kevinma40204275
24/8/19	7:07:20	bellanow1	24/8/19	20:07:08	kevinma40204275
24/8/19	5:32:56	bellanow1	24/8/19	19:32:51	kevinma40204275
24/8/19	4:32:56	bellanow1	24/8/19	15:07:24	kevinma40204275
24/8/19	0:07:31	bellanow1	24/8/19	13:32:55	kevinma40204275
			24/8/19	10:07:17	kevinma40204275
			24/8/19	7:32:54	kevinma40204275
			24/8/19	7:07:18	kevinma40204275
			24/8/19	5:32:54	kevinma40204275
			24/8/19	1:32:54	kevinma40204275

احتمال اینکه این ریتم دقیق فعالیت مربوط به یک انسان باشد بسیار کم است. این هماهنگی بین چندین حساب کاربری مختلف همراه با استفاده از عکس‌های گمراه‌کننده و جعلی نشان می‌داد که حساب‌ها به احتمال زیاد متعلق به اشخاص واقعی نیستند و به‌صورت خودکار فعالیت می‌کنند. با تجزیه و تحلیل الگوهای حساب‌های کاربری مشکوک مانند این حساب‌ها، استریک در نهایت به این نتیجه رسید که این حساب‌ها بخشی از یک شبکه ربات توئیتر حامی دولت اندونزی است که اطلاعات یک‌طرفه و گمراه‌کننده را در مورد درگیری در پاپوآی غربی منتشر می‌کند. (در مطالعه‌ی موردی فصل ۱۱-ب، «بررسی یک عملیات اطلاعاتی در پاپوآی غربی» ، در مورد شبکه‌ی بزرگ‌تری که این حساب‌ها بخشی از آن بودند، بیشتر بخوانید.)

بات چیست؟ پاسخ پیچیده‌تر از آن چیزی است که فکر می‌کنید.

پرونده‌ی پاپوآی غربی تنها عملیات اطلاعاتی‌ای نیست که از بات‌های شبکه‌های اجتماعی استفاده کرده است. سایر عملیات‌هایی از این نوع به‌طور گسترده‌تر مورد توجه و انتقاد قرار گرفته‌اند، اما شباهت‌هایی در نحوه‌ی عملکرد تمام این نوع عملیات‌ها وجود دارد.

بات یک برنامه‌ی نرم‌افزاری است که می‌تواند به‌طور خودکار وظایف محول‌شده توسط انسان را انجام دهد. خوب یا بد بودن یک ربات کاملا به نیات «صاحب» آن بستگی دارد.

بات‌هایی که اغلب در بحث‌های عمومی به آنها اشاره می‌شود، بات‌های اجتماعی هستند که در شبکه‌های اجتماعی از جمله فیس‌بوک، توئیتر و لینکدین فعال هستند. در این پلتفرم‌ها، می‌توان از آن‌ها برای انتشار پیام‌های ایدئولوژیک خاص استفاده کرد و هدف اغلب تظاهر به این است که موجی از حمایت از یک موضوع، شخص، قسمتی از یک محتوا یا هشتگ خاص وجود دارد.

بات‌های رسانه‌های اجتماعی را می‌توان به سه دسته‌ی اصلی تقسیم کرد: بات زمان‌بندی‌شده، بات تماشاگر و بات تقویت‌کننده. تشخیص این بات‌ها از هم مهم است چون هرکدام هدف، زبان و الگوی ارتباطی متفاوتی دارند. در زمینه‌ی اطلاعات نادرست، ما بیشتر با بات‌های تقویت‌کننده سروکار داریم.

کار بات تقویت‌کننده دقیقا همان چیزی است که از نامش برمی‌آید: تقویت و انتشار محتوا با هدف شکل‌دهی به افکار عمومی در فضای مجازی. همچنین با استفاده از این بات‌ها می‌توان تعداد دنبال‌کنندگان اشخاص و سازمان‌ها را بیش از تعداد واقعی آن‌ها جلوه داد. قدرت این بات‌ها ناشی از اعداد است. شبکه‌ای از بات‌های تقویت‌کننده می‌توانند تلاش کنند هشتگ‌ها را تحت تأثیر قرار دهند، لینک‌ها یا محتوای بصری را پخش کنند، هرزنامه‌های انبوه را به‌صورت گروهی ارسال کنند، یا فردی را به صورت آنلاین مورد آزار و اذیت قرار دهند، بدنامش کنند یا او را شخصیتی بحث‌انگیز و زیر فشار نشان دهند.

بات‌های تقویت‌کننده با کار هم‌زمان و در تعداد زیاد، موجه‌تر به نظر می‌رسند و بنابراین، به شکل‌گیری چشم‌انداز افکار عمومی آنلاین کمک می‌کنند. بات‌های تقویت‌کننده‌ای که اطلاعات نادرست را منتشر می‌کنند، این کار را عمدتاً از طریق کمپین‌های هشتگ یا با اشتراک‌گذاری اخبار در قالب لینک، ویدئو، میم، عکس یا انواع دیگر محتوا انجام می‌دهند. کمپین‌های هشتگ شامل بات‌هایی هستند که به‌طور مداوم یک هشتگ یا مجموعه‌ای از هشتگ‌ها را به‌صورت هماهنگ توئیت می‌کنند. هدف از این کار

اغلب فریب الگوریتم ترِند توئیتر برای افزودن یک هشتگ خاص به فهرست موضوعات پرطرفدار است. یک مثال هشتگ#Hillarysick است که پس از سکندری خوردن هیلاری کلینتون در سپتامبر ۲۰۱۶، کمی قبل از انتخابات ریاست جمهوری به‌طور گسترده توسط بات‌ها پخش شد. (همچنین مهم است توجه داشته باشید که کمپین‌های هشتگ نیازی به بات‌ها ندارند و می‌توانند بدون آن‌ها مؤثرتر باشند. این تحقیق در مورد «کارانه‌های هشتگ» انسانی در پاکستان را که توسط Dawn تهیه شده است ببینید.)

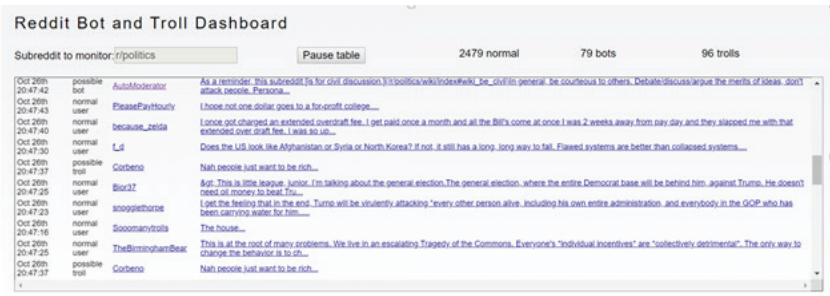
خرید و ایجاد ربات‌ها نسبتا آسان است. سایت‌های بی‌شماری هستند که ارتش ربات‌های خود را فقط با چندصد دلار یا حتی کمتر به شما می‌فروشند. اما ایجاد و نگهداری یک ربات اینترنتی پیچیده و شبیه به انسان بسیار سخت‌تر است.

نحوه‌ی تشخیص بات‌ها

دِولوپرها و محققان ابزارهای زیادی برای کمک به ارزیابی بات بودن یک حساب ساخته‌اند. این ابزارها می‌توانند در جمع‌آوری اطلاعات مفید باشند، اما نتیجه‌ی بررسی به کمک یک ابزار به هیچ وجه قطعی نیست و هرگز نباید تنها مبنای گزارش یا نتیجه‌گیری باشد.

یکی از شناخته‌شده‌ترین ابزارها Botometer است که توسط محققان دانشگاه ایندیانا ساخته شده است. این ابزار بر اساس معیارهای مختلف، احتمال اینکه یک حساب توئیتر و دنبال‌کنندگان آن بات باشند را محاسبه می‌کند.

جیسون اسکورونسکی برای وب‌سایت ردیت یک داشبورد زنده طراحی کرده است. زمانی که آن را برای کنترل یک ساب‌ردیت خاص تنظیم می‌کنید، به شما خواهد گفت نظرات توسط چه کسی ارسال شده، بات‌ها، ترول‌ها و یا انسان‌ها؟



اگرچه استثناهایی نیز وجود دارد، اما اکثر ابزارهای تشخیص بات‌ها که در دسترس عموم قرار دارند برای توئیتر ایجاد شده‌اند. دلیل این امر این است که بسیاری از شبکه‌های اجتماعی -از جمله فیس‌بوک- API (واسط برنامه‌نویسی کاربردی) خود را به گونه‌ای محدود می‌کنند که از تجزیه و تحلیل عمومی و استفاده از داده‌هایشان برای ایجاد چنین ابزارهایی جلوگیری شود.

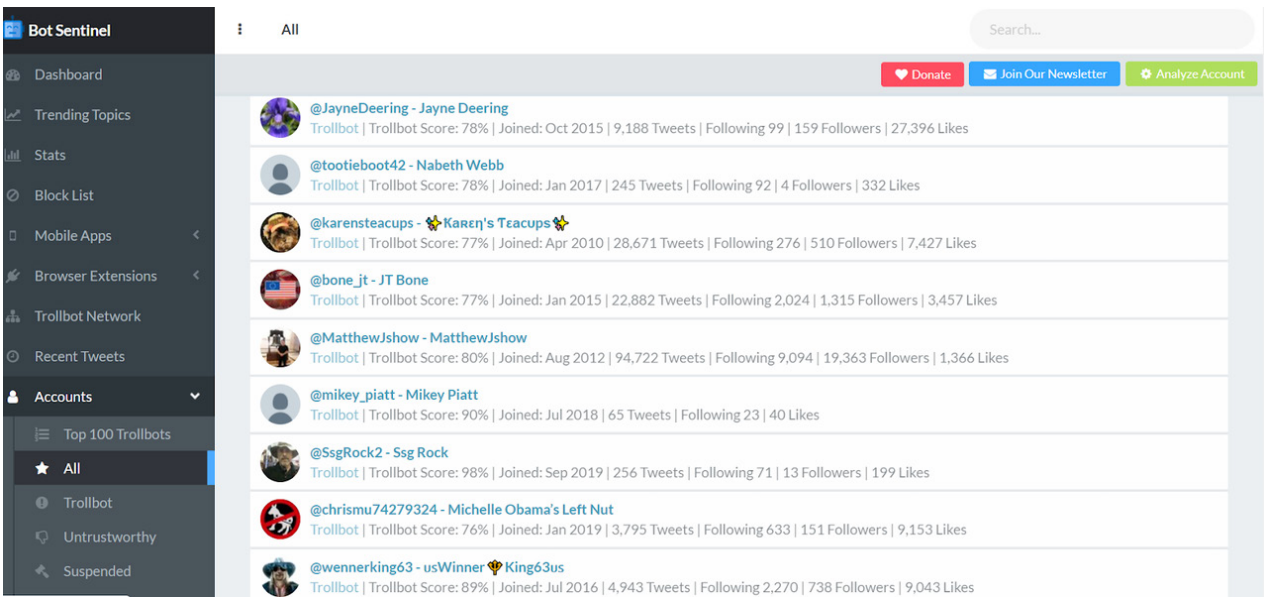
همانطور که قبلا هم اشاره کردیم، ابزارهای تشخیص بات نقطه‌ی شروع خوبی هستند اما نباید تنها مدرک شما باشند. یکی از دلایل تفاوت در میزان دقت آن‌ها این است که هیچ فهرست یگانه و کلی‌ای از تمام معیارها برای تشخیص بات‌ها با اطمینان صددرصد وجود ندارد. همچنین، بر سر اینکه دقیقا چه چیزی را می‌توان به‌عنوان بات طبقه‌بندی کرد نیز توافق وجود ندارد. محققان پروژه‌ی تبلیغات محاسباتی مؤسسه‌ی اینترنت آکسفورد حساب‌هایی که بیش از ۵۰ بار در روز پست می‌کنند را به عنوان حساب‌هایی با «اتوماسیون سنگین» طبقه‌بندی می‌کنند. آزمایشگاه تحقیقاتی دیجیتال فارنزیکس متعلق به شورای آتلانتیک، ۷۲ توئیت در روز (یک توئیت در هر ۱۰ دقیقه به مدت ۱۲ ساعت به‌صورت پیوسته) را مشکوک، و بیش از ۱۴۴ توئیت در روز را بسیار مشکوک قلمداد می‌کند.

تعیین اینکه آیا یک کمپین اطلاعات نادرست توسط بات‌های اجتماعی انجام می‌شود یا توسط انسان‌هایی که به انگیزه‌های مختلف، از جمله انگیزه‌های مالی، حجم زیادی از محتوا در مورد یک موضوع خاص را ارسال می‌کنند اغلب کار دشواری است. به‌عنوان مثال، بی‌بی‌سی دریافت حساب‌هایی که در نوامبر ۲۰۱۹ پیام‌های مشابهی در تقویت محتوای حامی بوریس جانسون در فیس‌بوک منتشر کرده‌اند، توسط افرادی مدیریت می‌شدند که وانمود می‌کردند بات‌های اجتماعی هستند.

گاهی نیز ممکن است با سایبورگ‌ها مواجه شوید، حساب‌های کاربری‌ای که تا حدی به‌صورت خودکار و تا حدی توسط انسان مدیریت می‌شوند و ترکیبی از رفتار طبیعی و غیرواقعی را نشان می‌دهند. روزنامه‌نگاران باید از زدن برچسب بات به حساب‌های مشکوک بدون شواهد و تحلیل مناسب خودداری کنند، زیرا اتهام اشتباه می‌تواند اعتبار شما را تضعیف کند.

یکی از راه‌های مقابله با انواع مختلف ربات‌ها، سایبورگ‌ها و حساب‌های انسانی بیش‌فعال این است که به جای تلاش برای شناسایی تنها یک نوع خاص از حساب مشکوک، تحقیقات خود را بر روی رصد کردن همه‌ی رفتارهای غیرواقعی یا ربات‌گونه متمرکز کنید.

به‌عنوان مثال، Bot Sentinel پایگاه داده‌ای شامل حساب‌های توئیتری (در ایالات متحده) که رفتار مشکوکی از خود نشان می‌دهند را در دسترس عموم قرار می‌دهد. سازندگان آن تصمیم گرفتند به جای جستجوی بات‌های اجتماعی، «حساب‌هایی که مکررا قوانین توئیتر را نقض می‌کردند» شناسایی و فهرست کنند.



مراحل بررسی فعالیت‌های غیرواقعی

به‌طور کلی، ما رویکرد زیر را برای شناسایی فعالیت‌های غیرواقعی و بالقوه خودکار در شبکه‌های اجتماعی پیشنهاد می‌کنیم:

۱. حساب‌ها را به‌صورت دستی برای فعالیت‌های مشکوک بررسی کنید.

۲. بررسی اولیه‌ی خود را با استفاده از ابزارها یا تحلیل‌های فنی‌تر شبکه ترکیب کنید.

۳. فعالیت‌ها، محتوا و شبکه‌ی سایر حساب‌هایی که با حساب‌های مشکوک تعامل دارند را بررسی کنید. این بررسی‌ها را با روش‌های سنتی‌تر تحقیق، مانند تلاش برای تماس با صاحب حساب یا افرادی که ادعا می‌کنند آنها را می‌شناسند، ترکیب کنید.

۴. با کارشناسان خارج از مؤسسه‌ی خود که در زمینه‌ی بات‌ها و فعالیت‌های غیرواقعی تخصص دارند، مشورت کنید.

برای اینکه بتوانید حساب‌های مشکوک را به‌صورت دستی بررسی کنید، آشنایی با علائم هشداردهنده‌ای که حکایت از خودکار بودن یک حساب کاربری در توئیتر و یا سایر شبکه‌های اجتماعی دارند مهم است.

هر بات رسانه‌ی اجتماعی نیاز به یک هویت دارد. سازندگان بات‌ها می‌خواهند حساب‌هایشان را تا حد امکان متقاعدکننده جلوه دهند، اما راه‌اندازی حساب‌های کاربری‌ای با ظاهر باورپذیر زمان می‌برد، به‌ویژه اگر هدف ایجاد یک شبکه‌ی بزرگ از بات‌ها باشد. هرچه یک نفر حساب‌های بیشتری داشته باشد، ایجاد و مدیریت آن‌ها به گونه‌ای که معتبر و باورپذیر به نظر برسند زمان بیشتری می‌برد. این همان جایی است که دست این حساب‌ها رو می‌شود. در بسیاری از موارد، سازندگان آن‌ها برای ایجاد یک حساب کاربری باورپذیر به حداقل‌ها اکتفا می‌کنند و یک محقق خوب می‌تواند این را تشخیص دهد.

بعضی از نشانه‌هایی که می‌توانید به دنبالشان باشید عبارتند از:

عکس حساب کاربری واقعی نیست

استفاده از عکس‌های جعلی و دزدیده‌شده و یا ایجاد حساب کاربری بدون عکس می‌تواند نشانه‌ای از عدم اصالت باشد. از آنجایی که سازندگان بات‌ها می‌خواهند حساب‌های زیادی را هم‌زمان ایجاد کنند، باید مجموعه‌ای از عکس‌ها تهیه کنند و اغلب آن‌ها را از وب‌سایت‌های دیگر کپی می‌کنند. بااین‌حال، چنین کاری ناهماهنگی‌هایی ایجاد می‌کند. به‌عنوان مثال، حساب کاربری‌ای که عکس یک مرد را دارد اما نام کاربری‌اش به‌گونه‌ای است که این شبهه را ایجاد می‌کند که حساب ممکن است متعلق به یک زن باشد، نشان از این دارد که که چیزی سر جایش نیست. برای حل این مشکل، بسیاری از سازندگان بات‌ها، کارتون‌ها یا عکس حیوانات را برای حساب کاربری خود انتخاب می‌کنند، اما در این‌صورت نیز این ترفند الگوی دیگری برای شناسایی حساب‌های غیرواقعی یا بات‌ها در اختیارمان قرار می‌دهد.

نام‌های کاربری‌ای که به صورت خودکار ایجاد شده‌اند

در مرحله‌ی بعد نام‌ها و نام‌های کاربری را بررسی کنید. هر نام کاربری‌ای در توئیتر منحصربه‌فرد است، به این معنی که نام کاربری‌ای که می‌خواهید انتخاب کنید اغلب اوقات قبلا توسط شخص دیگری استفاده شده است. این برای افراد عادی هم دردسرساز است، چه برسد به زمانی که بخواهید ۵۰، ۵۰۰، یا ۵هزار حساب کاربری در مدت زمانی کوتاه ایجاد کنید؛ آن وقت است که انتخاب نام‌های کاربری به یک چالش واقعی تبدیل می‌شود.

اما سازندگان ربات‌ها اغلب استراتژی‌ای را به کار می‌گیرند که به آن‌ها کمک می‌کند نام‌های کاربری بلااستفاده را به‌راحتی پیدا کنند. کدهایی با معیارهایی مانند موارد زیر برای ایجاد خودکار نام‌های کاربری استفاده می‌شوند:

Username followed by a 4 digit number	12 random characters in length which can consist of (a-zA-Z and 0-9)	Any first name followed by a random eight-digit number, indicating that the default username generated by Twitter has been used.
superman_1230 superman_2313 superman_9832 superman_3934 superman_4920	vP1tfI1ZoPG1 dNi29j2utANQ YQBrodhbPC84 TUq3R6GBWYyA XI87NreGshx8	Neil03121977 Sarah92839820 Claire02938593 John09340293 Stephen83749284

هنگامی که متوجه چندین حساب توئیتر با نام‌های کاربری‌ای می‌شوید که از تعداد حروف و ارقام یکسانی تشکیل شده‌اند، می‌توانید به صورت دستی حساب‌های بیشتری با آن الگو را در فهرست دنبال‌کنندگان حساب‌ها جستجو کنید و شبکه‌های بالقوه را شناسایی کنید.

در این مثال، حساب‌ها وجه اشتراک دیگری نیز دارند: همه‌ی آنها در سپتامبر ۲۰۱۹ ایجاد شده‌اند. وقتی این نکته با نشانه‌های دیگر ترکیب شود، می‌تواند نشان‌دهنده‌ی این باشد که همه‌ی حساب‌ها در یک زمان و توسط یک شخص ایجاد شده‌اند.

فعالیت حساب با طول عمر آن مطابقت ندارد

اگر یک حساب کاربری جدید تعداد نسبتاً زیادی دنبال‌کننده داشته باشد یا اگر در مدت کوتاهی تعداد زیادی توئیت منتشر کرده باشد، باید نسبت به آن مشکوک‌تر شوید. همین امر در صورتی که یک حساب کاربری قدیمی با وجود فعال بودن، دنبال‌کننده‌های کمی داشته باشد نیز صادق است.

اگر با چنین حساب کاربری‌ای مواجه شدید، فعالیتش را عمیق‌تر تحلیل کنید. تعداد توئیت‌های موجود را که در بالای صفحه آمده در نظر بگیرید و آن را بر تعداد روزهای فعال بودن حساب تقسیم کنید. به‌عنوان مثال، حسابی را در نظر بگیرید که تا تاریخ ۱۱ نوامبر ۲۰۱۹ دارای ۳۴۸۹ توئیت است و در ۱۵ آگوست ۲۰۱۹ ایجاد شده است. ۳۴۸۹ را بر ۸۹ تقسیم کنید (تعداد روزهایی که این حساب فعال بوده است) و نتیجه ۳۹.۲ توئیت در روز خواهد بود.

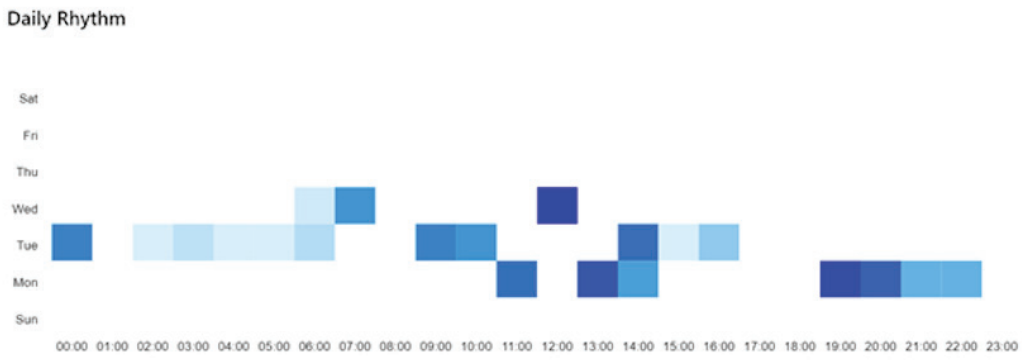
با نگاهی به توئیت‌های فرستاده شده در طول عمر حساب، آیا این تعداد بسیار زیاد، غیر واقعی یا نشدنی به نظر می‌رسد؟

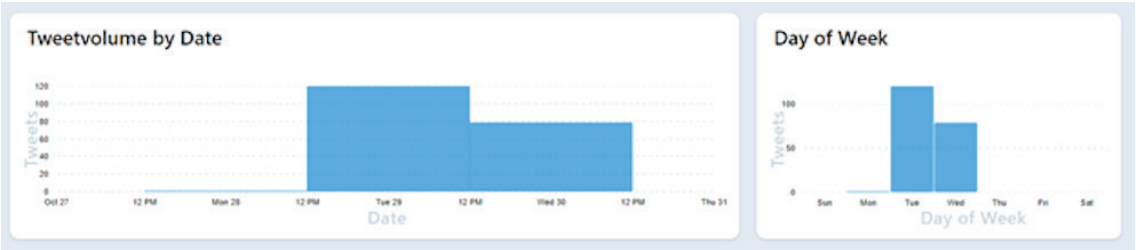
الگوهای توئیت مشکوک

عنصر دیگری که باید بررسی شود ریتم توئیت‌ها است. انسان‌ها ممکن است ترجیحات جزئی برای روزها و زمان‌هایی که معمولا توئیت می‌کنند داشته باشند، اما بعید است که فردی فقط در روزهای دوشنبه، سه شنبه و چهارشنبه به طور مداوم پست بگذارد و در تمام روزهای دیگر هفته و برای مدتی

طولانی کاملا سکوت کند.

برای مشاهده‌ی این الگوها در یک حساب کاربری خاص می‌توانید از ابزار تجزیه و تحلیل حساب که توسط لوکا هَمِر ساخته شده استفاده کنید:

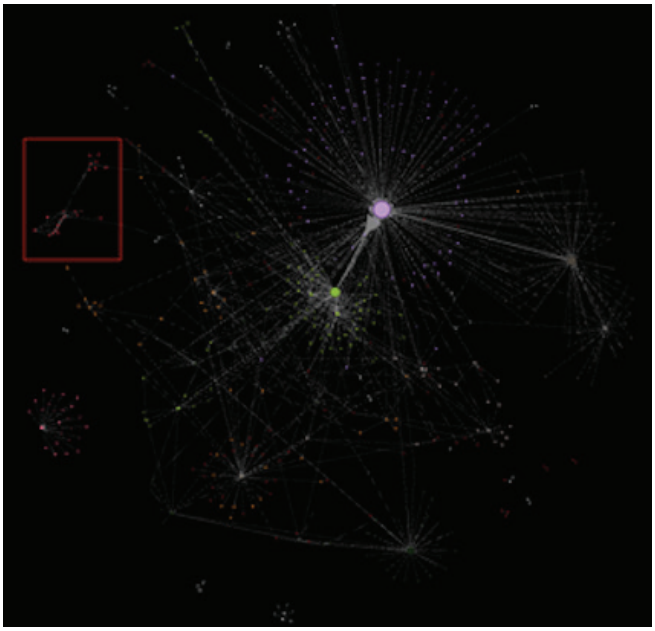




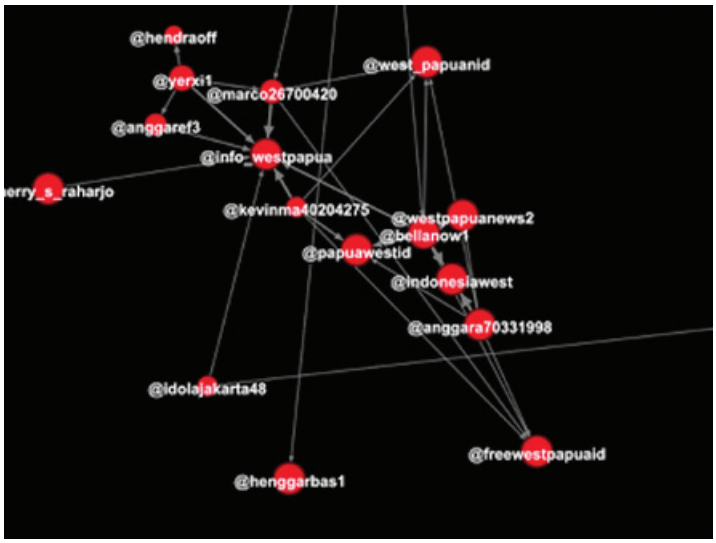
مصورسازی به‌عنوان بخشی از تحقیقات

برای درک بهتر فعالیت یک شبکه‌ی کامل از بات‌ها، می‌توانید از یک پلتفرم مصورسازی مانند Gephi استفاده کنید. بنجامین استریک، همکار بلینگ‌کت، از این ابزار برای تجزیه و تحلیل ارتباطات بین حساب‌های توئیتر متعلق به شبکه‌ی بات حامی دولت اندونزی استفاده کرد.

با نگاهی به نمایش بصری ارتباطات بین تعداد زیادی از حساب‌های توئیتر، استریک متوجه شد که ساختار سمت چپ تصویر (به رنگ قرمز) با باقی تصویر تفاوت‌هایی دارد.



با بزرگنمایی در این بخش از تصویر، او می‌توانست ببیند کدام حساب‌های توئیتر بخشی از این ساختار خاص هستند.



هر دایره‌ی قرمزرنگ یک حساب توئیتر را نشان می‌دهد و خطوط، نشانگر روابط بین آن‌ها هستند. معمولا حساب‌های کوچک‌تر حول یک دایره‌ی بزرگ‌تر در وسط جمع می‌شوند، به این معنی که همه

آن‌ها با حساب تأثیرگذار تعامل دارند. بااین‌حال، حساب‌های موجود در ساختار بالا به این شکل با یکدیگر تعامل نداشتند. این امر استریک را تشویق کرد به تجزیه و تحلیل فعالیت‌های آن حساب‌های غیرعادی بپردازد.

آینده‌ی بات‌های اجتماعی: آیا می‌توانیم آن‌ها را فریب دهیم؟

فناوری بات‌های اجتماعی در چند سال اخیر بسیار پیشرفته‌تر شده است و به این نرم‌افزارهای کوچک اجازه می‌دهد رفتار انسان‌ها را ماهرانه‌تر شبیه‌سازی کنند. در حال حاضر به نقطه‌ای رسیده‌ایم که بسیاری پیش‌بینی می‌کنند کاربران مصنوعی می‌توانند در ارتباطات آنلاین پیچیده شرکت کنند، بدون اینکه همتایان انسانی‌شان متوجه شوند که درواقع در حال گفتگوی طولانی با یک بات هستند.

با این حال، تاکنون هیچ مدرکی وجود ندارد که نشان دهد ربات‌های اجتماعی سطح بالایی که از ویژگی قدرتمند یادگیری ماشین برخوردار باشند در حال پا گرفتن هستند.
دکتر اوله پوتز، محقق پروژه‌ی «ربات‌های بی‌طرفی که پل می‌سازند» از دانشگاه بیله‌فیلد آلمان می‌گوید: «فکر نمی‌کنم ربات‌های اجتماعی پیچیده‌ی زیادی وجود داشته باشند که بتوانند با مردم مکالمه‌ی واقعی برقرار کرده و آن‌ها را به پذیرش مواضع سیاسی خاصی ترغیب کنند.» به گفته‌ی او، بهترین راه برای کمک به مردم برای تشخیص فعالیت‌های غیرواقعی در شبکه‌های اجتماعی، استفاده از روش تشخیصی است که همه‌ی عواملی را که یک حساب کاربری را مشکوک می‌کنند فهرست‌بندی کرده و بسنجد. به‌عنوان مثال، او می‌گوید: «یک حساب ممکن است از دستورالعمل خاصی استفاده کند که اخبار را بازنشر و به‌طور خودکار دیگران را دنبال می‌کند، درحالیکه حساب غیرواقعی دیگری ممکن است این ویژگی را داشته باشد که هیچ‌گاه از الگوهای گفتاری‌ای که معمولاً توسط انسان‌ها استفاده می‌شود، استفاده نمی‌کند».
در حال حاضر، تجزیه و تحلیل روشمند فعالیت‌ها، محتوا، تعاملات و الگوهای تکرارشونده‌ی یک حساب کاربری بهترین رویکرد برای شناسایی فعالیت‌های غیرواقعی است.
در فصل مربوط به مطالعه‌ی موردی‌مان، توضیحات عمیق‌تر و فنی بیشتری درباره‌ی نحوه‌ی تحلیل این عوامل مختلف درباره‌ی شبکه‌ای مشکوک در توئیتر، که با اعتراضات هنگ‌کنگ مرتبط بود، را ارائه خواهیم کرد.

۳.الف. مطالعه‌ی موردی: یافتن شواهدی از فعالیت‌های خودکار در توئیتر در طول اعتراضات هنگ‌کنگ

نوشته‌ی: جوانا وایلد و شارلوت گدار

شارلوت گدار محقق و مدرس بِلینگ‌کَت است. پیش از انتقال به بلینگ‌کت او در مرکز حقوق بشر دانشگاه برکلی، کالیفرنیا فعالیت می‌کرد. وی در برکلی در آزمایشگاه تحقیقاتی کار می‌کرد و درعین‌حال وظیفه‌ی آموزش دانشجویان برای انجام تحقیقات با استفاده از داده‌های منبع‌باز در مورد درگیری‌های جهانی برای نهادهای بشردوستانه‌ی بین‌المللی را بر عهده داشت.

جوانا وایلد محقق داده‌های منبع‌باز در بلینگ‌کت است. او همچنین بر توسعه‌ی فناوری و ابزار برای تحقیقات دیجیتال نیز تمرکز دارد. او سابقه‌ی روزنامه‌نگاری آنلاین را نیز دارد و پیش از این در مناطق (پسا)درگیری با روزنامه‌نگاران کار کرده است. یکی از نقش‌های او حمایت از روزنامه‌نگاران در شرق آفریقا برای تولید برنامه جهت پخش در صدای آمریکا بود.

در آگوست ۲۰۱۹، توئیتر اعلام کرد که هزاران حساب کاربری که به گفته‌ی آن به انتشار اطلاعات نادرست در مورد اعتراضات هنگ‌کنگ کمک کرده و بخشی از «عملیاتی هماهنگ با حمایت دولت» بودند، را حذف کرده است. به زودی، فیس‌بوک و یوتیوب نیز با انتشار بیانیه‌هایی گفتند که حساب‌هایی که شامل فعالیت‌های غیرواقعی هماهنگ در مورد اعتراضات بودند را حذف کرده‌اند.

برخلاف فیس‌بوک و یوتیوب، توئیتر فهرستی از حساب‌های حذف‌شده منتشر کرد و فرصتی برای بررسی بیشتر این فعالیت‌ها فراهم کرد. تیم ما، به همراه یکی از شرکت‌کنندگان در کارگاه بلینگ‌کت، تصمیم گرفت محتوای باقی‌مانده در توئیتر در مورد اعتراضات در هنگ‌کنگ را بررسی کند تا نشانه‌هایی از فعالیت‌های غیرواقعی هماهنگ را شناسایی کند.

پیدا کردن فعالیت‌های مشکوک

ما کار خود را با جستجوی هشتگ‌های مرتبط با اعتراضات شروع کردیم. یک جستجوی ساده با کلمات کلیدی «شورش‌های هنگ‌کنگ» توئیت‌های زیادی را نشان می‌داد که برخی حاوی هشتگ‌های متعدد بودند.

هدف ما این بود که بر روی حساب‌ها و محتوای حامی چین تمرکز کنیم، زیرا این‌ها همان حساب‌هایی بودند که توئیتر قبلا فعالیت‌های غیرواقعی‌شان را شناسایی کرده بود. ما کلمات کلیدی مورد نظرمان را به این ترتیب فرمول‌بندی کردیم:

Shame on Hong Kong" -police government"

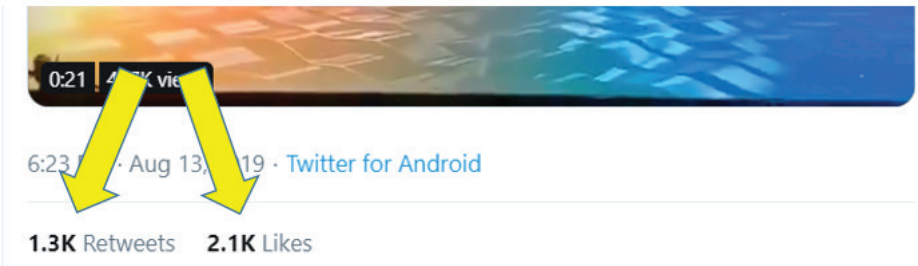
"شرم بر هنگ‌کنگ"-پلیس-دولت

این جستجو نتایجی را به دست می‌دهد که حاوی عبارت "شرم بر هنگ کنگ" باشند، اما حاوی کلمات پلیس یا دولت نباشند. هدف این بود که توئیت‌هایی مانند "شرم بر پلیس هنگ‌کنگ" حذف شوند و توئیت‌هایی مانند "شرم بر معترضان هنگ‌کنگی" باقی بمانند. سایر عبارات جستجو شامل «سوسک‌های هنگ‌کنگی» و «اوباش هنگ‌کنگی» می‌شد؛ صفات رایج برای معترضان هنگ‌کنگی که توسط حساب‌های توئیتر حامی چین استفاده می‌شدند.

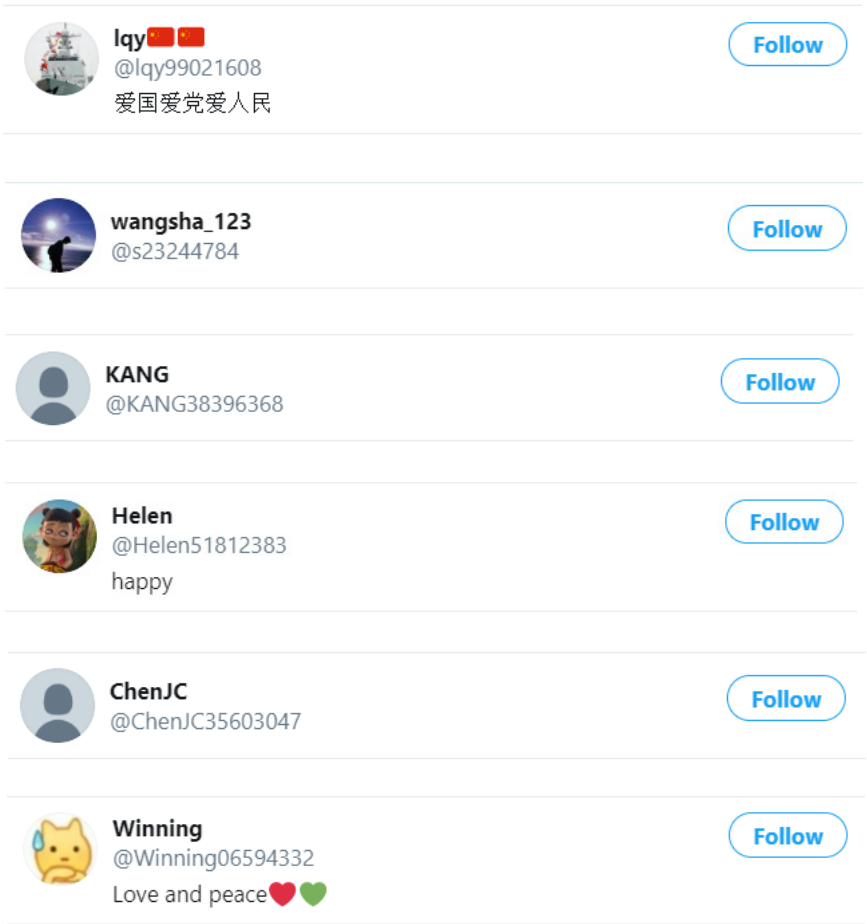
پس از جستجو با استفاده از این عبارات و عبارات مشابه دیگر، به سراغ توئیت‌های اخیر درباره‌ی هنگ‌کنگ رفتیم که ریتوئیت‌ها و لایک‌های زیادی دریافت کرده بودند. می‌توانید به‌سادگی با افزودن"min_retweets:500" یا "min_faves:500" به عبارت جستجوی خود، نتایج را براساس میزان تعاملات غربال کنید. این عبارت‌های جستجو فقط توئیت‌هایی با حداقل ۵۰۰ ریتوئیت یا لایک را به دست خواهند داد.

سپس به سراغ حساب‌های کاربری‌ای رفتیم که با آن توئیت‌ها تعامل داشتند. به‌عنوان مثال، توئیتی از طرف کاربر تأییدشده، شیجین هو، وجود داشت که سردبیر نسخه‌ی چینی و انگلیسی گلوبال تایمز، یک رسانه‌ی دولتی چین، است:

سپس روی لینک ریتوئیت‌ها و لایک‌ها در کنار هر عدد کلیک کردیم و فهرست حساب‌هایی که محتوا را ریتوئیت یا لایک کرده بودند بررسی کردیم.



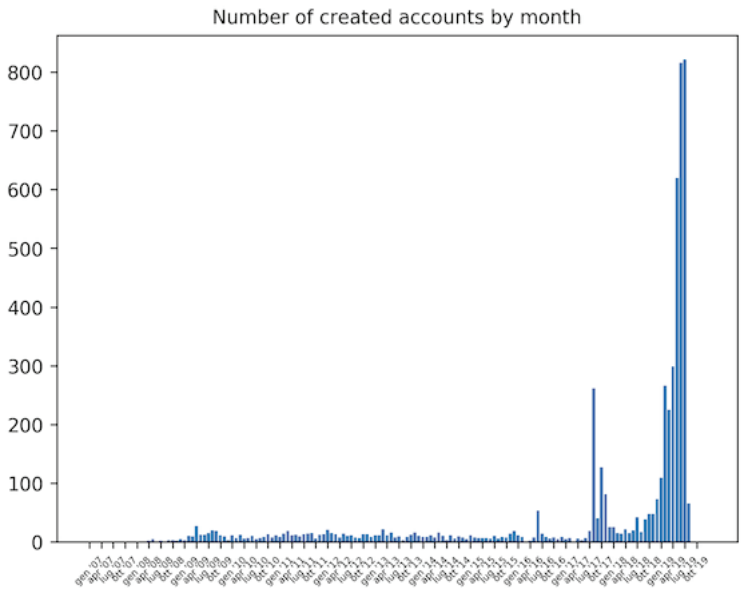
فرضیه‌ی ما این بود که حساب‌های غیرواقعی حامی چین توئیت‌های پرسنل برجسته‌ی رسانه‌ی دولتی چین را تقویت می‌کنند. ما متوجه شدیم که بسیاری از نام‌های کاربری در فهرست ریتوئیت‌ها و لایک‌ها متمایز بودند، چراکه شامل یک عدد هشت‌رقمی بعد از نام بودند که نشان می‌داد کاربر هنگام ثبت‌نام نام کاربریِ پیش‌فرض تولیدشده توسط توئیتر را پذیرفته است.



با بررسی این حساب‌ها متوجه شدیم که همه‌ی آن‌ها دنبال‌کننده‌های معدودی دارند و خود نیز حساب‌های معدودی را دنبال می‌کنند، توضیحی از خود در بیوگرافی‌شان ارائه نداده‌اند، تا حد زیادی فقط توئیت‌های دیگران را ریتوئیت می‌کنند و خودشان توئیتی ندارند و تقریبا تمام محتوایی که ریتوئیت می‌کنند در مخالفت با اعتراضات است.

ما همچنین متوجه شدیم که تاریخ ایجاد این حساب‌ها بسیار جدید و حدود آگوست ۲۰۱۹ است. از آنجایی که توئیتر فهرستی از حساب‌های حامی چین را که حذف کرده بود منتشر کرد، می‌توانستیم تاریخ ایجاد آن حساب‌ها را بررسی کنیم و ببینیم آیا روند مشابهی را نشان می‌دهند یا نه.

با کمک لوئیجی گوبِلو، کدنویسی که در جامعه‌ی منبع‌باز آنلاین فعالیت دارد، از یک اسکریپت ساده‌ی پایتون (می‌توانید کد مورد استفاده‌ی او را در GitHub و اطلاعات بیشتر درباره‌ی او را اینجا پیدا کنید) برای شناسایی الگوهای موجود در داده‌ها استفاده کردیم. نمودار زیر نشان می‌دهد که حساب‌های حذف‌شده همگی در ماه‌های اخیر ایجاد شده بودند که با ویژگی‌های مجموعه‌حساب‌های فعال مورد بررسی ما مطابقت داشت.



خودکار کردن فرآیند جستجو

بعد از اینکه موفق شدیم مجموعه‌ای از حساب‌ها با ویژگی‌ها و فعالیت‌های مشکوک را شناسایی کنیم، تصمیم گرفتیم تجزیه و تحلیلمان را گسترده‌تر کنیم. این کار مستلزم خودکار کردن بخشی از روند جستجو بود. یکی از شرکت‌کنندگان در کارگاه بلینگ‌کت که سابقه‌ای در توسعه‌ی نرم‌افزار داشت یک قطعه‌ی کوچک کد جاوا اسکریپت با عبارت باقاعده‌ی (\w+\d{8\})- برای انجام دو عملکرد نوشت:

استخراج نام‌های کاربری حساب‌هایی که توئیت خاصی را ریتوئیت یا لایک کرده بودند. و سپس غربال کردن فهرست نام‌های کاربری به‌گونه‌ای که این نام‌ها فقط مطابق با یک الگوی خاص در فهرست باقی بمانند. الگویی که او برای عملکرد دوم انتخاب کرد، نام‌هایی بود که با یک عدد ۸ رقمی همراه باشند.

با بارگیری این اسکریپت در کنسول ابزارهای ویژه‌ی توسعه‌دهندگان در گوگل کروم، که ابزارهای توسعه‌دهنده‌ی وب را مستقیما در مرورگر ارائه می‌کند، هر زمان که روی لینک ریتوئیت‌ها یا لایک‌های یک توئیت خاص کلیک می‌کرد، اسکریپت در پس‌زمینه اجرا می‌شد. نتایج به دست آمده نام‌هایی را که با الگوی موردنظر مطابقت داشتند برجسته می‌کرد. برای دیدن نمونه‌ی نتایج به اینجا بروید.

ما توانستیم با استفاده از این اسکریپت حساب‌های کاربری‌ای را که با توئیت‌های مهم حامی چین تعامل داشتند بررسی کنیم. در بحبوحه‌ی اعتراضات هنگ‌کنگ، لیو ییفئی، بازیگر آمریکایی‌چینی، پستی در Weibo در حمایت از پلیس به اشتراک گذاشت که باعث شد برخی افراد در شبکه‌های اجتماعی خواهان تحریم فیلم جدید او، مولان شوند. بااین‌حال، متوجه شدیم که بسیاری از حساب‌های توئیتر از این بازیگر و فیلمش با استفاده از هشتگ #SupportMulan حمایت می‌کنند. (سی‌ان‌ان نیز در این مورد گزارشی تهیه کرده است). ما تصمیم گرفتیم از این اسکریپت برای بررسی کاربرانی که توئیت‌های حامی مولان را ریتوئیت یا لایک کرده‌اند استفاده کنیم.

به‌این‌ترتیب، نام‌های حساب‌هایی را که با الگوی ما مطابقت داشتند جمع‌آوری کرده و تاریخ ساختشان را بررسی کردیم. مشخص شد که بیشتر این حساب‌های کاربری در ۱۶ آگوست ایجاد شده‌اند.

https://twitter.com/monicaG62882882	created: 16 August, 20.07h
https://twitter.com/Min85741833	created: 16 August, 05.29h
https://twitter.com/cherry71737735	created: 16 August, 19.22h
https://twitter.com/Catheri57246362	created: 16 August, 06.13h
https://twitter.com/crystal09837022	created: 16 August, 04.16h
https://twitter.com/Suqing26464572	created: 16 August, 06.30h
https://twitter.com/Yates52905656	created: 16 August, 22.16h
https://twitter.com/hu02261927/	created: 16 August, 04.53h
https://twitter.com/xinjin66947005	created: 16 August, 19.18h
https://twitter.com/Ta99869608	created, 16 August, 21.15h

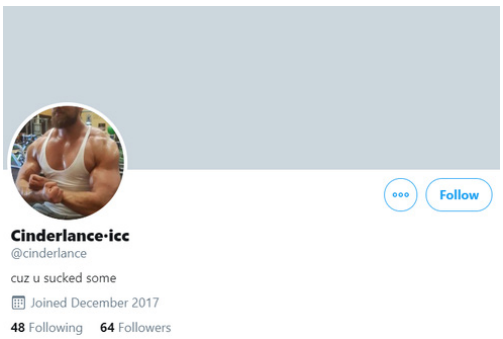
همانطور که در زیر نشان داده شده است، تاریخ و زمان دقیق ایجاد حساب‌ها را با نگه داشتن نشانگر ماوس روی اطلاعات پیوستن (joined) به دست آوردیم:

بعد از اینکه موفق شدیم مجموعه‌ای از حساب‌های خاص را شناسایی کنیم، تجزیه و تحلیل دستی محتوایی را که آن‌ها به اشتراک گذاشته بودند آغاز کردیم. به سرعت مشخص شد که حساب‌های موجود در فهرست ما همگی به نفع ییفئی (Yifei) و علیه معترضان هنگ‌کنگ توئیت کرده‌اند.

بسیاری از حساب‌های موجود در فهرست ما پس از ۱۷ یا ۱۸ آگوست غیرفعال شده بودند، که باز هم نشان‌دهنده‌ی نوعی هماهنگی بود. دقیقا نمی‌دانیم چرا این حساب‌ها غیرفعال شدند، اما احتمال دارد توئیتر برای ورود از سازندگان حساب‌ها تأییدات بیشتری درخواست کرده باشد که آن‌ها قادر به ارائه‌اش نبوده‌اند. توضیح دیگر می‌تواند این باشد که سازندگان حساب‌ها نمی‌خواستند پس از اینکه توئیتر شروع به تعلیق حساب‌های حامی چین کرد، سوءظن بیشتری را به خود جلب کنند.

اما چند ماه بعد متوجه شدیم که تعداد زیادی از این حساب‌های کاربری دوباره فعال شده‌اند. این بار آن‌ها پیام‌هایی در حمایت از ییفئی و فیلم او، مولان پخش کردند.

ما همچنین موفق شدیم حساب‌های کاربری دیگری پیدا کنیم که حامی مولان بودند و درعین حال همگی دارای نام‌های کاربری‌ای با الگوی خاص و تاریخ ایجاد مشابه بودند و مرتبا پیام‌هایی در حمایت از ییفئی منتشر می‌کردند. این کار را از طریق جستجوی هشتگ‌هایی مانند #SupportMulan و #liuyifei انجام دادیم.



اینطور که به نظر می‌رسد این حساب‌ها، شاید برای جلوگیری از مسدود شدنشان توسط توئیتر، استراتژی خود را از انتقاد از معترضان هنگ‌کنگی به حمایت از بازیگر زن و فیلمش تغییر داده‌اند.

این مطالعه‌ی موردی نشان می‌دهد که چگونه می‌توان تکنیک‌های دستی و خودکار را برای کشف سریع شبکه‌ای از حساب‌های توئیتر مشکوک با هم ترکیب کرد. همچنین نشان می‌دهد که جستجوی حساب‌ها و فعالیت‌های بیشتری با اهداف مشابه، حتی پس از اعلام حذف بعضی حساب‌ها توسط یک پلتفرم، می‌تواند مفید باشد.

در اینجا، ما توانستیم از تکنیک‌های ساده‌ی جستجو و جزئیات حساب‌ها برای شناسایی مجموعه‌ی بزرگی از حساب‌ها استفاده کنیم که مشخصا برای فعالیت‌های هماهنگ و غیرواقعی استفاده می‌شدند.

۴. تشخیص اخبار جعلی و عملیات اطلاعاتی در موقعیت‌های خبری فوری

نوشته‌ی: **جین لیتوینکو**

جین لیتوینکو گزارشگر ارشد بازفید نیوز است و حوزه‌ی اصلی کارش دروغ‌پراکنی‌ها، امنیت سایبری و تحقیقات آنلاین است. او پیش از این موفق شده است کمپین‌های دستکاری اطلاعات در شبکه‌های اجتماعی، کلاهبرداران ارزهای دیجیتال و عاملان بدی که با اهداف مالی به انتشار اطلاعات نادرست می‌پردازند را ردیابی و کشف کند. او همچنین در زمان‌های بحران اطلاعاتی را که بناست طیف وسیعی از مخاطبان از آن‌ها استفاده کنند را راستی‌آزمایی می‌کند. جیم اصالتا اهل کیف اوکراین است و در حال حاضر در تورنتوی کانادا اقامت دارد.

وقتی اخبار فوری در مورد حادثه یا رویدادی منتشر می‌شود، ممکن است ساعت‌ها یا حتی روزها طول بکشد تا مقامات و خبرنگاران بتوانند کاملا موقعیت را درک کنند. با شکل گرفتن جریان شواهد و جزئیات اولیه در شبکه‌های اجتماعی و دیگر پلتفرم‌های آنلاین، عاملان بد فضای مجازی می‌توانند برای ایجاد نفاق و چنددستگی، پاشیدن بذر بی‌اعتمادی و به جیب زدن مبلغی پول از رهگذر توجه مصرف‌کنندگانِ نگران، وارد عمل شوند. بعضا نیز همین مصرف‌کنندگان خوش‌نیت یا سایر منابع می‌توانند ناخواسته اطلاعات نادرست یا گمراه‌کننده را منتشر کنند. وجود ترکیبی از احساسات شدید و جریان آهسته‌ی انتشار اخبار در دقایق و ساعات اولیه‌ی یک رویداد، یعنی روزنامه‌نگاران باید به ابزار و تکنیک‌های لازم برای رصد مؤثر، راستی‌آزمایی و - در مواقع لزوم - افشای اخبار فوری جعلی مجهز باشند. ایجاد یک توئیت، عکس، حساب رسانه‌ی اجتماعی یا مقاله‌ی جعلی فقط چند دقیقه طول می‌کشد و اطلاعات واقعی به‌سختی می‌تواند با این روند پرسرعت رقابت کند.

کلید ردیابی و افشای اخبار فوری جعلی این است که قبل از وقوع چنین رویدادهایی روزنامه‌نگاران دانش پایه‌ی خود را برای مدیریت این موقعیت‌ها تقویت کرده باشند. این یعنی داشتن مهارت‌های پایه‌ی لازم در درستی‌سنجی (از جمله مهارت‌هایی که در اولین کتابچه‌ی راهنمای راستی‌آزمایی به آن‌ها اشاره شده است)، درک نحوه‌ی رصد کردن شبکه‌های اجتماعی، و آشنایی با نحوه‌ی پاسخگویی مناسب

در صورتی که خود یا همکارانتان توسط عاملان بد فضای مجازی هدف قرار بگیرید. خبرنگاران همیشه باید ایمنی آنلاین را در اولویت قرار دهند.

اولین گام پس از انتشار اخبار فوری شناسایی جوامعی است که تحت تأثیر واقعه قرار گرفته‌اند. در جریان تیراندازی سال ۲۰۱۸ در دبیرستان پارکلند، فلوریدا، خبرنگاران شروع به جستجوی نقشه‌ی اسنپ‌چت برای یافتن فیلم‌هایی کردند که وضعیت دانش‌آموزان گیرافتاده در کلاس‌ها را نشان می‌داد. در مقابل، در طول طوفان ایرما در سال ۲۰۱۷، تمرکز بر فیس‌بوک، جایی که افراد آسیب‌دیده سعی می‌کردند اطلاعات دریافت کنند، بسیار مهم‌تر بود. درک چگونگی عملکرد هر شبکه‌ی اجتماعی و چگونگی تلاقی آن با یک رویداد معین ضروری است.

این فصل بر ابزارهایی تمرکز می‌کند که خبرنگاران می‌توانند برای رصد و افشای اخبار فوری جعلی از آن‌ها استفاده کنند. هر ابزاری برای هر موقعیتی مناسب نیست و درک اینکه چه کسی تحت تأثیر یک رویداد خاص قرار گرفته است می‌تواند کمکتان کند تشخیص بدهید باید روی کدام ابزارها بیشتر تمرکز کنید.

سه چیزی که باید دنبالش بگردید

همانطور که خبرنگاران و پلتفرم‌های مختلف برای مقابله با اخبار نادرست و دروغ‌پراکنی تلاش می‌کنند، عاملان بد نیز مشغول بهبود بخشیدن ترفندهای خود برای ناشناس ماندن هستند. بااین‌حال، بعضی الگوهای ثابت رفتار و فعالیت همچنان به چشم می‌خورند:

۱.تصاویر دستکاری‌شده و تحریف‌شده

تصویری از یک کوسه که در بزرگراهی سیل‌زده در حال شنا کردن است مدت‌ها است که دست‌به‌دست می‌شود و مردم را فریب می‌دهد (یکی از مطالعات موردی اولین کتابچه‌ی راهنمای راس نیز به همین موضوع اختصاص داشت). عکس‌ها و ویدئوهایی که جعلی بودنشان پیش از این افشاء شده و راستی‌آزماها و افشاکنندگان آن‌ها را فریب‌های زامبی می‌نامند باید حتما رصد شوند. در مقایسه با متن، تصاویر بسیار سریع‌تر در فضای مجازی پخش می‌شوند و به همین دلیل تمرکز بر آن‌ها اغلب سودبخش است.

در جریان تیراندازی در ال‌پاسو در والمارت در سال ۲۰۱۹، شخصیت‌های راست افراطی تلاش کردند یک ویدئوی قدیمی یوتیوب را که به مظنون مرتبط نبود، با عنوانی دیگر جا زده و از آن سوء استفاده کنند.

۲. قربانی‌ها یا مجرمان جعلی

در جریان تیراندازی در دفتر مرکزی یوتیوب، شبکه‌های اجتماعی مملو از ادعاهای نادرست درباره‌ی مظنونان بود. در طول انتخابات میان‌دوره‌ای ایالات متحده در سال ۲۰۱۸، شایعات نادرستی مبنی بر رأی دادن مهاجران غیرقانونی توسط رئیس‌جمهور ایالات متحده منتشر شد. سروکله‌ی مجرمان دروغین در اکثر رویدادهای خبری بزرگ پیدا می‌شود.

در جریان تیراندازی پارکلند در سال ۲۰۱۸، یک حساب کاربری جعلی با نام بیل اورایلی تلاش کرد نامی دروغین از مظنون پخش کند.

۳. آزار و اذیت در فضای مجازی و لشگرکشی

اگرچه این دقیقا مصداق پراکندن اطلاعات نادرست نیست، اما بسیار اتفاق می‌افتد که عاملان بد برای وادار کردن افراد درگیر در یک واقعه‌ی خبری به سکوت، به آزار و اذیت آن‌ها می‌پردازند. این امر همچنین نشان از آن دارد که توجه گروهی از افراد به یک واقعه‌ی خاص جلب شده است و ممکن است بعدا از ترفندهای مختلفی در رابطه با این رویداد استفاده کنند. «بریگِیدینگ» یا لشگرکشی به وضعیتی گفته می‌شود که در آن عده‌ای از افراد با هم دست‌به‌یکی می‌کنند تا از طریق اعمالی مثل بالا یا پایین بردن امتیازها در رأی‌دهی به یک محتوا و کامنت‌باران کردن یک کاربر خاص، توهم وجود یک جنبش یا واکنش تندگستر عمومی را ایجاد کنند.

پس از مناظره‌ی رهبری دموکرات‌ها در سال ۲۰۱۹، حساب‌های ناشناس پیام مشابهی را در مورد نژاد کامالا هریس منتشر کردند.

بهترین روش‌های بایگانی و انتشار

قبل از شروع جستجو، یک پوشه برای اسنادتان ایجاد کنید و یک صفحه‌گسترده (spresdsheet) هم برای آنچه پیدا خواهید کرد در نظر بگیرید. به محض پیدا کردن حقه‌ها از آن‌ها اسکرین‌شات بگیرید و صفحه‌ی مورد نظر را بایگانی کنید (می‌توانید برای این کار از افزونه‌ی مرورگر وب Archive.org که یک ابزار رایگان، سریع و مؤثر برای بایگانی محتوا است استفاده کنید). مطمئن شوید URLهای اصلی و بایگانی‌شده را در صفحه‌گسترده‌ی خود ثبت می‌کنید. به این طریق در آینده و بعد از اینکه آب‌ها از آسیاب افتاد، می‌توانید به سراغ شواهدی که جمع کرده‌اید برگردید.

برای جلوگیری از کمک به انتشار صفحات مرتبط با اطلاعات نادرست یا دروغین، مطمئن شوید که به جای آدرس اصلی، به URL آرشیوشده در مقالات یا پست‌های رسانه‌های اجتماعی لینک می‌دهید. همچنین بهترین روش این است که تصاویر خود را با یک برچسب واضح مانند «نادرست» یا «گمراه‌کننده» واترمارک کنید تا مطمئن شوید که در زمینه‌ی مناسبی پخش و ذخیره می‌شوند. اگر قصد نوشتن مقاله دارید، تمرکز تیتر و متن خود را به جای چیزهایی که نادرستند، بر اطلاعات درست بگذارید. مطالعات نشان داده است که تکرار دروغ‌ها می‌تواند باعث شود اطلاعات نادرست در مغز افراد جا بیافتد.

نقش ما جلوگیری از تکرار شدن دروغ‌ها تا حد امکان و هدایت مردم به سمت اطلاعات دقیق و درست است.

شناسایی کلمات کلیدی و مکان‌ها

همانطور که جزئیات بیشتری از واقعه آشکار می‌شود، فهرستی از کلمات کلیدی و مکان‌های مرتبط با واقعه برای خودتان تهیه کنید. در ارتباط با مکانْ نام شهر، ایالت/استان و کشور و همچنین هرگونه نام مستعاری را که برای محله یا شهر آسیب‌دیده استفاده می‌شود، یادداشت کنید. در طول انتخابات باید نام شهرستان‌ها و حوزه‌های انتخاباتی را نیز ثبت کنید. این اطلاعات برای رصد پست‌های دارای برچسب جغرافیایی و جستجوی موارد اشاره به مکان خاص استفاده می‌شود. همچنین مطمئن شوید که حساب‌های اجتماعی مقامات محلی مربوطه، مانند پلیس و آتش‌نشانی، سیاستمداران و

خبرگزاری‌های محلی را شناسایی کرده‌اید، و شروع به رصد کردن آن‌ها کنید.

گام بعدی شناسایی کلمات کلیدی است. این می‌تواند شامل کلماتی مانند قربانی، مظنون، تیرانداز، تیراندازی، سیل، آتش، نام‌های تأییدشده‌ی افراد درگیر و عبارات کلی‌تر مانند "در جستجوی" باشد. علاوه بر کلمات کلیدی، به عبارت‌ها و سایر عناصر زبانی‌ای فکر کنید که افراد ممکن است در چنین موقعیت‌هایی به کار ببرند. اگر حساب معتبری را پیدا کردید که ادعا می‌کند در دل واقعه حضور دارد، نام کاربری‌اش را یادداشت کنید و تمام محتواهایی را که در فیدش وجود دارد بخوانید. برای پیدا کردن افراد دیگری در منطقه که ممکن است تحت تأثیر واقعه قرار گرفته باشند می‌توانید فهرست دوستان یا دنبال‌کنندگان این کاربر معتبر را بررسی کنید.

توجه داشته باشید که افراد ممکن است در موقعیت‌های پراسترس املای نام‌ها و نام مکان‌ها را اشتباه بنویسند. به‌عنوان مثال، در طول آتش‌سوزی کین‌کِید در کالیفرنیا در سال ۲۰۱۹، به دلیل مشکلات تصحیح خودکار عده‌ای به جای املای Kincade، #Kinkaid را توئیت کرده بودند. اشتباهات رایج املایی را در جستجوهایتان بگنجانید و سعی کنید با تایپ کردن عبارات کلیدی در دستگاه خود و مشاهده‌ی پیشنهادهایی که ظاهر می‌شوند، اشتباهات احتمالی تصحیح خودکار را شناسایی کنید.

همچنین، این مقطع زمان خوبی است تا با هر منبعی که در مکان مربوطه می‌شناسید و یا با کسانی که بخشی از جوامعی هستند که ممکن است مورد آزار و اذیت یا هدف اطلاعات نادرست قرار بگیرند، تماس بگیرید و از آن‌ها درباره‌ی آنچه در فضای مجازی دیده‌اند پرس‌وجو کنید. می‌توانید به مخاطبان خود بگویید که سعی دارید اطلاعات نادرست و سایر محتوای مشکل‌ساز مرتبط با رویداد را شناسایی کنید. با تیم رسانه‌های اجتماعی اتاق خبر خود هماهنگ کنید تا خبر جستجوی اخبار نادرست توسط شما را منتشر کنند و ببینید آیا آن‌ها چیز قابل توجهی دیده‌اند یا خیر.

ابزارهای مرتبط با تصاویر

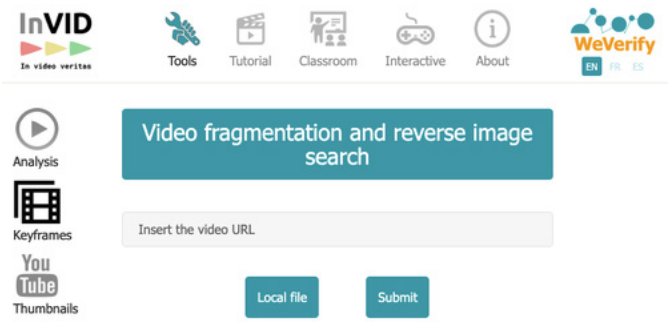
۱. جستجوی عکس

جستجوی معکوس عکس یکی از ابزارهای ضروری است. برای جستجوی یک تصویر در گوگل، می‌توانید روی آن کلیک‌راست و گزینه‌ی "Search Google for Image" را در مرورگر کروم انتخاب کنید. اما بهتر است همیشه تصاویر را با استفاده از چند ابزار مختلف جستجو کنید. اگر افزونه‌ی مرورگر InVID را نصب کنید، می‌توانید روی یک تصویر کلیک‌راست و آن را در ابزارهای مختلف جستجو کنید. این نمودار مقایسه‌ی جستجوی معکوس عکس که توسط Domain Tools ایجاد شده، نقاط قوت و ضعف محصولات مختلف جستجوی معکوس تصویر را نشان می‌دهد:

	Elements Identified	Faces	Structures	Places	Digital/ Logos	Alternate Sizes	Flipped or Altered
Google	1	Neutral	Great	Great	Great	Good	Neutral
Yandex	2+	Great	Great	Great	Good	Good	Good
Bing	3+	Good	Good	Good	Good	Neutral	Great
TinEye	1	Neutral	Neutral	Neutral	Great	Great	Good

InVID

InVID یک افزونه‌ی رایگان مرورگر و بهترین پلتفرم برای کمک به تجزیه و تحلیل و درستی‌سنجی ویدئوها است. این افزونه به کاربران اجازه می‌دهد URL مورد نظر خود را در موتور جستجوی InVID وارد کرده و سپس تصاویر کوچکی را از ویدئو استخراج کنند. به‌این‌ترتیب می‌توانید با جستجوی معکوس عکس‌هایی که به دست آورده‌اید ببینید این ویدئو در کجای وب ظاهر شده است.



۲. جستجو با استفاده از TweetDeck

بهترین ابزار برای جستجو در توئیتر TweetDeck است که به شما این امکان را می‌دهد ستون‌های منحصربه‌فردی برای جستجوها و فهرست‌ها ایجاد کنید.

پیدا کردن و کپی کردن فهرست‌های مرتبط کلیدی یکی از مهم‌ترین راه‌ها برای همگام حرکت کردن با اطلاعاتی است که به تدریج درباره‌ی یک واقعه منتشر می‌شود. با استفاده از یک فرمول ساده می‌توانید از گوگل برای جستجوی فهرست‌های توئیتر استفاده کنید. این عبارت را در موتور جستجوی خود تایپ کنید: site:twitter.com/*/lists. سپس یک کلمه‌ی کلیدی را با علامت نگارشی نقل‌قول به آن اضافه کنید؛ مثلا "Alabama reporters". رشته‌ی جستجوی نهایی به این شکل خواهد بود: "site:twitter.com/*/lists "Alabama reporters

این جستجو هر فهرستی که توسط کاربران توئیتر ایجاد شده و در عنوان آن گزارشگران آلاباما آمده باشد را نشان خواهد داد.

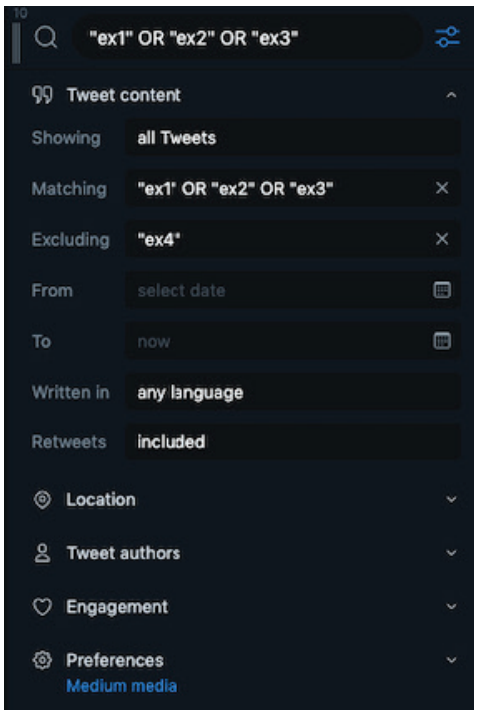
هنگامی که فهرستی را که با نیازهای شما منطبق است پیدا کردید، باید آن را کپی کنید تا بتوانید آن را در TweetDeck وارد کنید.

برای این کار می‌توانید از این برنامه استفاده کنید:

http://projects.noahliebman.net/listcopy/connect.php

می‌توانید هر تعداد فهرست که مایل باشید را کپی کنید. این برنامه بیشتر برای کپی کردن فهرست‌های ایده‌ال است تا دنبال کردن آن‌ها زیرا می‌توانید کاربران را به دلخواه خود اضافه یا حذف کنید.

علاوه بر پیدا کردن و اضافه کردن فهرست‌های توئیتر به ستون‌های TweetDeck، باید ستون‌هایی با فیلترهای جستجوی خاص هم ایجاد کنید که کمک کند کلمات کلیدی، تصاویر و ویدئوها را به‌سرعت جستجو کنید. برای جستجوی چندین کلمه‌ی کلیدی، آن‌ها را در علامت نقل‌قول بگذارید و با واژه‌ی «OR» از هم جدایشان کنید؛ به‌عنوان مثال "Kincade" OR "Kinkade". همچنین می‌توانید کلماتی را که نتایج غیرمرتبط با اهداف جستجوی شما می‌آورند، حذف کنید. افرادْ دیگر به‌ندرت توئیت‌های خود را بر اساس مکان برچسب‌گذاری می‌کنند. بنابراین، می‌توانید این قسمت را خالی بگذارید و به‌این‌ترتیب، دامنه‌ی جستجوی خود را گسترش دهید.



اگر می‌خواهید نتایج جستجوی خود را محدود کنید، گزینه‌ی From را بر روی یک یا دو روز قبل از واقعه تنظیم کنید تا مطمئن شوید بعضی توئیت‌ها را به دلیل اختلاف زمانی از دست نمی‌دهید. اگر باز هم تعداد نتایج نمایش‌داده‌شده زیاد بود، می‌توانید این بار نتایج را با استفاده از گزینه‌ی تعامل‌ها فیلتر کنید تا مطمئن شوید فقط توئیت‌هایی را مشاهده می‌کنید که ریتوئیت یا لایک شده‌اند.

همچنین، می‌توانید عبارات کلیدی را به ستون‌های جداگانه تقسیم کنید. به‌عنوان مثال، مکان‌ها را در یک ستون و کلمات کلیدی دیگر را در ستون دیگر قرار دهید. من معمولا ستون سومی را نیز برای اسامی احتمالی مظنونان یا قربانیان و غلط‌های املایی آن‌ها ایجاد می‌کنم. درنهایت، اگر حجم بسیار زیادی توئیت را مشاهده می‌کنید بهتر است ستونی از بهترین کلمات کلیدی خود ایجاد کنید و سپس با انتخاب گزینه‌ی "Showing" در بخش "Tweet Content" فقط عکس‌ها و ویدئوها را مشاهده کنید. این کار کمکتان می‌کند تصاویر پربازدید را شناسایی کنید.

۳. CrowdTangle

CrowdTangle یک برنامه و افزونه‌ی مرورگر است که به‌صورت رایگان در اختیار اتاق‌های خبر قرار دارد (اگر اتاق خبر شما به این برنامه دسترسی ندارد، با شرکت تولیدکننده‌ی آن تماس بگیرید).
این ابزار قدرتمند به شما امکان می‌دهد داشبوردهایی را برای رصد کردن فیس‌بوک، اینستاگرام و ردیت تنظیم کنید. شما همچنین می‌توانید اطلاعات مورد نیاز خود را بر اساس کلمات کلیدی جستجو کرده و محتوا را به شیوه‌های مختلفی از جمله زمان ارسال، زبان و تعامل غربال کنید. برنامه CrowdTangle به‌ویژه برای رصد فیس‌بوک و بررسی مکان‌هایی که ممکن است یک URL در رسانه‌های اجتماعی پست شده باشد مفید است.

پس از دسترسی، برای شروع به app.crowdtangle.com بروید و سپس روی "Create New Dashboard" کلیک کنید. حتی اگر به برنامه دسترسی نداشته باشید، استفاده از افزونه‌ی مرورگر برای همه رایگان است.

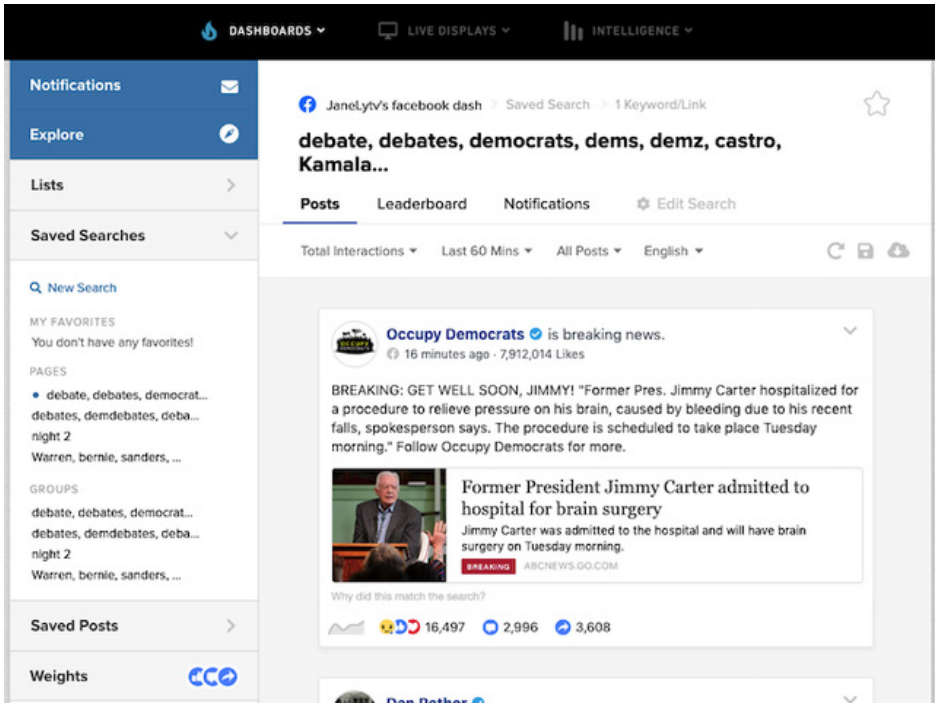
CrowdTangle: جستجوی پست‌های فیس‌بوک

روی گزینه‌ی "Saved Searches" در حاشیه‌ی سمت چپ صفحه کلیک کنید و سپس گزینه‌ی "New Search" را انتخاب کنید. برای جستجوی فیس‌بوک دو گزینه دارید: جستجو در صفحات و جستجو در گروه‌ها. توصیه‌ی من این است که هر دو را امتحان کنید. هر تعداد کلمه‌ی کلیدی که می‌خواهید وارد کرده و آن‌ها را با ویرگول از هم جدا کنید. سپس می‌توانید نحوه‌ی مشاهده‌ی پست‌ها را تنظیم کنید، به‌عنوان مثال بر اساس زمان ارسال، محبوبیت و عملکرد بیشتر از حد معمول، یعنی پست‌هایی است که تعامل دریافتی‌شان نسبت به پست‌های عادی همان صفحه‌ی خاص بیشتر است. بسته به موقعیت، من انتخاب خود از این سه گزینه را تغییر می‌دهم تا مطمئن شوم هم پست‌های پربازدید و هم جدیدترین پست‌ها را می‌بینم.

همچنین می‌توانید پست‌ها را بر اساس بازه‌ی زمانی و نوع خاص آن‌ها مرتب کنید.
CrowdTangle اخیرا امکان جستجوی پست‌ها بر اساس مکان صفحه‌ای که توسط آن پست شده‌اند را اضافه کرده است.

به‌عنوان مثال، با کلیک بر روی "English" و سپس انتخاب "Country"، می‌توانید فقط پست‌های صفحاتی را که مکانشان را ایالات متحده اعلام کرده‌اند انتخاب کنید. همچنین می‌توانید برعکس عمل کنید و پست‌هایی را که از صفحات مستقر در ایران، روسیه، عربستان سعودی، فیلیپین یا هند می‌آیند جستجو کنید. به پست‌های مبتنی بر تصویر و ویدئو توجه ویژه‌ای داشته باشید، چراکه سریع‌تر منتشر می‌شوند و جذابیت بیشتری برای کاربران دارند.

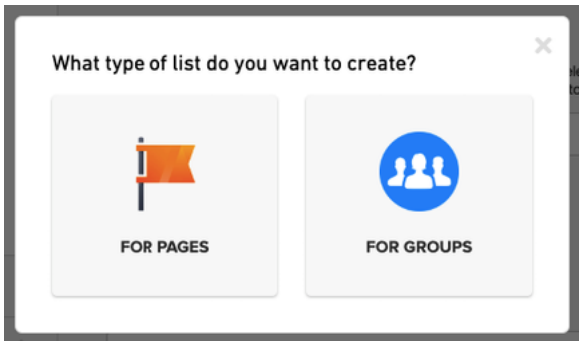
هنگامی که جستجوی مورد نظر خود را تنظیم کردید، حتما نتایج آن را ذخیره کنید تا بتوانید مدام به آن بازگردید.



CrowdTangle: فهرست‌ها

CrowdTangle هم مانند، TweetDeck به شما این امکان را می‌دهد که فهرستی از صفحات و گروه‌های عمومی مورد علاقه‌ی خود ایجاد کنید. با کلیک کردن بر روی گزینه‌ی "Lists" در حاشیه‌ی

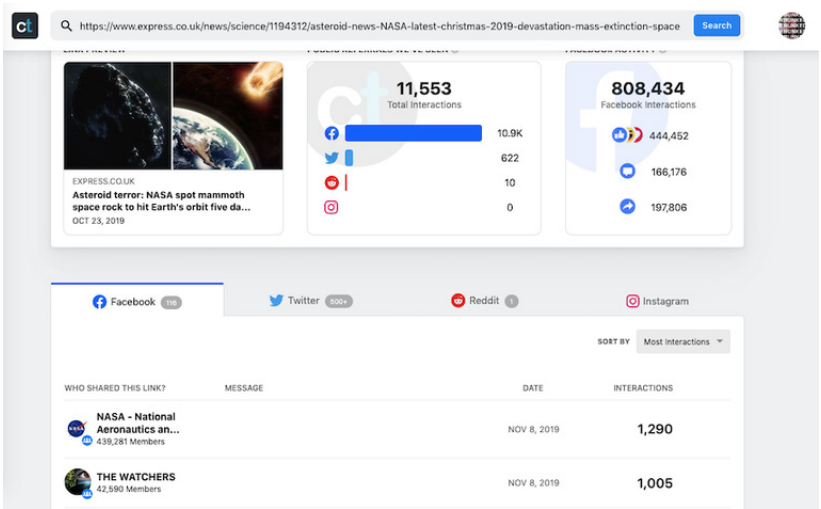
سمت چپ صفحه و سپس انتخاب گزینه‌ی "Create List" می‌توانید گروه‌هایی را که با کلمات کلیدی شما مطابقت دارند و یا صفحاتی را که URL آن‌ها را در اختیار دارید رصد کنید. CrowdTangle همچنین فهرست‌های پیش‌ساخته‌ای نیز دارد که می‌توانید با کلیک کردن بر روی گزینه‌ی "Explore" آن‌ها را مشاهده کنید. مانند توئیتر، اینجا نیز ایجاد فهرستی از صفحات و گروه‌هایی که در مورد رویدادی که شما آن را پوشش می‌دهید، صحبت می‌کنند، راه خوبی برای نظارت بر محیط اطلاعاتی است.



CrowdTangle: جستجوی لینک‌ها

یکی دیگر از ویژگی‌های مفید CrowdTangle امکان جستجوی لینک‌ها یا همان پیوندها است. به https://apps.crowdtangle.com/search بروید و URL یا عبارات کلیدی محتوای مورد نظرتان را وارد کنید. CrowdTangle مهم‌ترین موارد به اشتراک‌گذاری عمومی لینک در فیسبوک، اینستاگرام، ردیت و توئیتر را به شما نشان خواهد داد (توجه داشته باشید که نتایج مربوط به توئیتر محدود به هفت روز گذشته هستند). این کار به شما کمک می‌کند بفهمید محتوا چگونه در حال منتشر شدن است، آیا گروه‌ها یا افرادی وجود دارند که باید بیشتر در موردشان تحقیق کنید، و اینکه آیا محتوا به اندازه‌ای گسترش یافته است که نیاز باشد دست‌به‌کار شده و نادرستی آن را نشان بدهید؟ هیچ قاعده‌ی ساده‌ای در مورد اینکه چه زمانی باید اطلاعات نادرست را بی‌اعتبار کنیم وجود ندارد، اما چند سؤال خوب که می‌توانید از خودتان بپرسید این‌ها است: آیا این اطلاعات در خارج از شبکه‌ی اولیه‌ی اشتراک‌گذاران خود منتشر شده است؟ آیا توسط مقام شناخته‌شده‌ای به اشتراک گذاشته شده است؟

آیا این محتوا تعامل قابل توجهی ایجاد کرده است؟ (افزونه‌ی مرورگر این برنامه همان داده‌های ابزار جستجوی لینک را ارائه می‌دهد، و استفاده از هر دوی آن‌ها برای همه، حتی کسانی که یک حساب کاربری کامل در CrowdTangle ندارند، رایگان است).



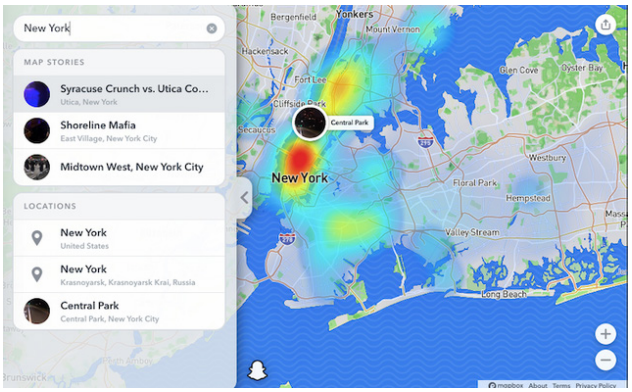
۴. Instagram.com

اینستاگرام فضای مفیدی برای رصد کردن هشتگ‌ها و پست‌های دارای برچسب جغرافیایی است. مکان‌های مرتبطی را که کاربران ممکن است در عکس‌هایشان برچسب‌گذاری کرده باشند جستجو کنید، و به یاد داشته باشید که برچسب‌های مکان می‌توانند محله‌ها و مکان‌های دیدنی و خاص را نیز شامل شوند. هنگامی که شخصی را پیدا کردید که به نظر می‌رسد در یک رویداد خبری شرکت داشته است، روی حسابش کلیک کنید و مطمئن شوید که استوری‌هایش را تماشا می‌کنید استوری‌ها در حال حاضر بسیار محبوب‌تر از پست‌های معمولی اینستاگرام هستند. همچنین، در بخش نظرات به دنبال سایر شاهدان احتمالی بگردید و هر هشتگ جدیدی که ممکن است در کنار پست‌های آن‌ها استفاده شده باشد را یادداشت کنید. اگر می‌خواهید استوری اینستاگرام شخصی را برای پوشه‌ی بایگانی خود دانلود کنید، می‌توانید از سایت‌هایی مانند storysaver.net برای دانلود آن استفاده کنید.

۵. SnapMap

وجود اطلاعات نادرست در اسنپ‌چت چندان معمول نیست، اما نقشه‌ی عمومی آن برای کمک به تایید اطلاعات یا بی‌اعتبار کردن اطلاعات نادرست مفید است.

برای شروع به map.snapchat.com بروید و مکان مورد نظر خود را وارد کنید. به‌این‌ترتیب نقشه‌ی حرارتی‌ای را خواهید دید که به شما نشان می‌دهد محتوای مورد نظر کجا در حال پخش شدن است؛ هرچه رنگ مکان روی نقشه‌ی حرارتی روشن‌تر باشد، اسنپ‌های بیشتری از آنجا در حال ارسال است. برای ذخیره‌ی اسنپ‌های مفید، روی سه نقطه در بالا سمت راست کلیک کنید و گزینه‌ی "Share" را انتخاب کنید. از این طریق می‌توانید URL اسنپ مورد نظر را کپی کنید تا بعدا در صورت نیاز به سراغش بروید (بهتر است از اسنپ مورد نظرتان یک اسکرین‌شات هم بگیرید).



همه‌چیز را کنار هم بگذارید

لازم است استفاده از تمام این ابزارها را از قبل تمرین کنید تا در موقعیت‌های خبری فوری گیج نشوید و اشتباه نکنید. اطلاعات نادرست اغلب احساسات افراد را هدف می‌گیرند و از خلأها و شکاف‌های موجود در اطلاعات استفاده می‌کنند. هنگام جستجو باید این نکته را در نظر داشته باشید. همچنین،

اغلب با اطلاعات دقیقی مواجه می‌شوید که می‌تواند به همکارانتان کمک کند. همه‌ی اطلاعات دقیق و صحیحی که پیدا می‌کنید را یادداشت کنید تا بتوانید مطالب نادرست را سریع‌تر تشخیص دهید، و از کمک گرفتن از دیگر خبرنگاران رسانه‌تان که در محله حادثه حضور دارند نترسید.

مرور دوباره‌ی عکس‌ها و پست‌هایی که ذخیره کرده‌اید بعد از اینکه آب‌ها از آسیاب افتاد می‌تواند مفید باشد. در لحظه‌ی وقوع یک رویداد احتمالا می‌خواهید با اطلاعات نادرست منفردی که مشاهده می‌کنید مقابله کنید، اما پس از تمام شدن ماجرا می‌توانید به دنبال الگوها و فعالیت‌های هماهنگ بگردید. آیا افراد به دلیل نژاد یا جنسیت خود هدف قرار گرفته بودند؟ آیا حقه‌هایی که از حساب‌های کوچک و ناشناس شروع شده بودند به جریان اصلی تبدیل شدند؟ آیا هیچ یک از رسانه‌های اجتماعی عملکردی خاصه خوب یا ضعیف داشتند؟ یک خلاصه‌داستان می‌تواند به خوانندگانتان کمک کند به طور کامل هدف و روش انتشار اطلاعات نادرست را درک کنند. همچنین این کار می‌تواند ابزار مناسبی برای شما و اتاق خبرتان باشد و به شما نشان دهد در موقعیت‌های بعدی اخبار فوری، تمرکز بر روی چه مواردی می‌تواند مفید باشد.

۵. بررسی و تأیید تصاویر

نوشته‌ی: هانا گای، فریدا ویس، سایمون فاکنر

فریدا ویس مدیر «ویژوال سوشال لب» و استاد رسانه‌های دیجیتال در دانشگاه متروپولیتن منچستر است. در دانشگاه و همچنین در حوزه‌ی روزنامه‌نگاری داده‌محور تمرکز او بر چگونگی گسترش اطلاعات نادرست در فضای مجازی است. وی در شورای دستور کار جهانی رسانه‌های اجتماعی در مجمع جهانی اقتصاد (۲۰۱۳ تا ۲۰۱۶) و شورای جهانی آینده‌ی اطلاعات و سرگرمی (۲۰۱۶ تا ۲۰۱۹) فعالیت کرده و از مدیران اُپن دِیتا در منچستر نیز هست.

سایمون فاکنر مدرس تاریخ هنر و فرهنگ بصری در دانشگاه متروپولیتن منچستر است. تحقیقات او به کاربردهای سیاسی و معانی تصاویر، با تمرکز ویژه بر کنشگری و جنبش‌های اعتراضی مربوط می‌شود. او نیز یکی از مدیران ویژوال سوشال مدیا لب است و علاقه‌ی زیادی به توسعه‌ی روش‌های مرتبط با تجزیه و تحلیل تصاویر منتشرشده در رسانه‌های اجتماعی دارد.

هانا گای دانشجوی دکترای دانشگاه متروپولیتن منچستر است که به بررسی نقش تصاویر در انتشار اطلاعات نادرست در شبکه‌های اجتماعی پرداخته است. او نیز یکی از اعضای ویژوال سوشال مدیا لب است. پروژه‌های فعلی او در این سازمان شامل مطالعه‌ی تصاویر به‌اشتراک‌گذاشته‌شده در توئیتر در طول کمپین «جان سیاه‌پوستان ارزشمند است» و همچنین، سواد رسانه‌ای بصری برای مقابله با اطلاعات نادرست در مدارس کانادا است.

امروزه قسمت اعظم ارتباطات در رسانه‌های اجتماعی بصری است. عکس‌ها و ویدئوها به راحتی توجه کاربران را جلب می‌کنند، متقاعدکننده هستند، ساختن آن‌ها از هر زمانی ساده‌تر است و می‌توانند واکنش‌های احساسی قدرتمندی را ایجاد کنند. در نتیجه، آنها به ابزارهای قدرتمند انتشار اطلاعات نادرست و دروغ‌پراکنی تبدیل شده‌اند.

تا به امروز، بحث در مورد تصاویر در زمینه‌ی اطلاعات نادرست و دروغ‌پراکنی یا بر تکنیک‌های راستی‌آزمایی متمرکز بوده و یا اخیرا بیشتر بر روی ویدئوهای جعلی و دیپ‌فِیک متمرکز شده است. ما

در فصل بعد به مقوله‌ی دیپ‌فیک‌ها خواهیم پرداخت، اما پیش از آن لازم است با بعضی از ترفندهای ساده‌تر تولید عکس‌ها و ویدئوهای جعلی -خصوصا آن‌هایی که در جایی خارج از زمینه‌ی رویدادشان استفاده می‌شوند- آشنا شویم.

با توجه به استفاده‌ی گسترده از تصاویر برای تحریک و دستکاری گفتمان عمومی، روزنامه‌نگاران باید به دانش بنیادی برای راستی‌آزمایی تصاویر مجهز باشند و بتوانند تصاویر را با دیدی نقادانه بررسی و ارزیابی کنند و به پرسش‌هایی از این دست پاسخ بدهند که چرا و چگونه از تصاویر برای هدفی خاص استفاده شده است. این فصل بر توسعه‌ی این دسته‌ی دوم از مهارت‌ها تمرکز دارد و از چارچوبی استفاده می‌کند که ما در ویژوال سوشال مدیا لب ایجاد کرده‌ایم.

استفاده از راستی‌آزمایی

در ویژوال سوشال مدیا لب، تمرکز ما بر درک نقش‌هایی است که تصاویر فضای مجازی در جامعه ایفا می‌کنند. اگرچه تمرکز ما بیشتر بر تصاویر ثابت (Still Images) است، کارمان به‌صورت کلی طیف گسترده‌تری از تصاویر را در بر می‌گیرد: عکس‌ها، تصاویر ترکیبی (Composite Images)، میم‌ها، تصاویر گرافیکی و اسکرین‌شات‌ها. مقابله با اطلاعات نادرست و دروغ‌های بصری مستلزم به‌کارگیری مجموعه‌ای از استراتژی‌های خاص خود است. تا به امروز، راستی‌آزمایی تصویر توسط روزنامه‌نگاران بر این موضوع متمرکز بوده است که آیا تصویر همان چیزی است که آن‌ها تصور می‌کنند یا خیر.

تروشار بارُت در ویرایش اول کتابچه‌ی راهنمای راستی‌آزمایی چهار اصل اساسی برای راستی‌آزمایی تصاویر بیان کرده است که همچنان بسیار ارزشمند هستند. راهنمای راستی‌آزمایی بصری فرست درفت نیز منبع مفید دیگری است که این اصول را با تمرکز بر پنج سؤال درباره‌ی عکس‌ها و ویدئوها به کار می‌بندد:

۱. آیا نسخه‌ای که می‌بینید نسخه‌ی اصلی عکس است؟

۲. آیا می‌دانید عکس توسط چه کسی گرفته شده است؟

۳. آیا می‌دانید عکس کجا گرفته شده است؟

۴. آیا از زمان گرفته شدن عکس اطلاع دارید؟

۵. آیا می‌دانید عکس به چه دلیل گرفته شده است؟

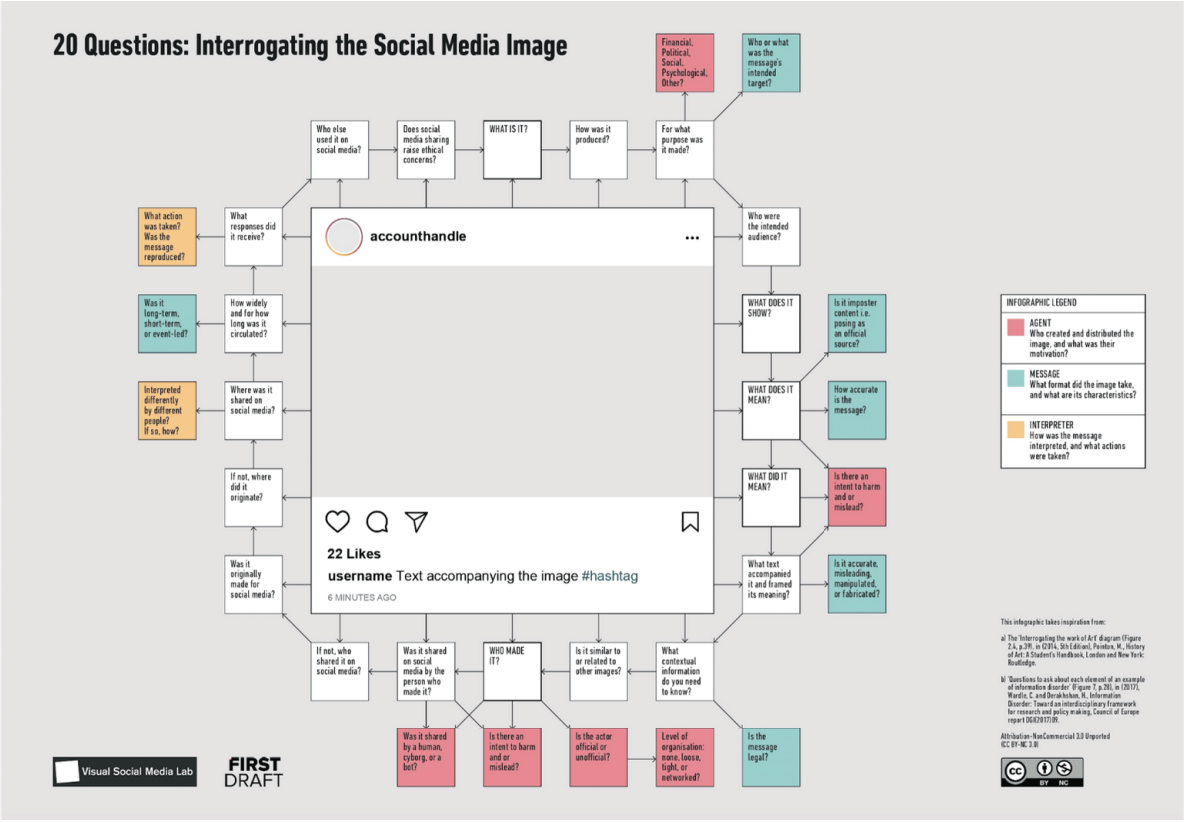
ابزارهای استانداردی که می‌توانید برای بررسی عکس‌ها و ویدئوها از آن‌ها استفاده کنید عبارتند از:

InVID، جستجوی عکس TinEye ،Yandex، جستجوی عکس Google و Forensically. این ابزارهای صحت‌سنجی بر منشأ تصویر تمرکز می‌کنند.

اگرچه استفاده از این ابزارها همچنان اهمیت زیادی دارد، در عین حال استراتژی‌ها و تکنیک‌هایی که اغلب در کمپین‌های اطلاعات نادرست و دروغ‌پراکنی‌ها و در طیفی از اشکال دستکاری‌های رسانه‌ای استفاده می‌شوند هم برای بررسی اینکه تصاویر چگونه و توسط چه کسی استفاده و به اشتراک گذاشته می‌شوند مهم‌اند، همچنین نقش احتمالی خبرنگاران در تقویت بیشتر تصاویر مشکل‌دار را نشان می‌دهد.

برای فراتر رفتن از اَشکال استاندارد تأیید تصاویر، ما روش‌هایی از مطالعات تاریخ هنر را با سؤالاتی که مخصوصا برای محتوای نادرست و دروغ‌پراکنی طراحی شده‌اند ترکیب کرده‌ایم. طرح راستی‌آزمایی ما به نام بیست سوال برای بررسی تصاویر در رسانه‌های اجتماعی، که با همکاری فرست درفت و همکاران خبرنگارمان طراحی شده است، یکی دیگر از ابزارهایی است که روزنامه‌نگاران می‌توانند هنگام بررسی تصاویر از آن استفاده کنند.

بررسی تصاویر شبکه‌های اجتماعی



همانطور که از عنوان این قسمت مشخص است، طرح ما شامل ۲۰ پرسش است که می‌توان در مورد هر تصویری در رسانه‌های اجتماعی (تصویر ثابت، ویدئو، گیف، و غیره) پرسید، به همراه ۱۴ سؤال دیگر با هدف کاوش بیشتر در جنبه‌های مختلف اطلاعات نادرست و دروغ‌پراکنی. سؤالات ترتیب مشخصی ندارند، اما بهتر است بررسی‌های خود را با پنج سؤال زیر شروع کنید:

۱. این تصویر چیست؟

۲. چه چیزی را نشان می‌دهد؟

۳. چه کسی آن را ساخته است؟

۴. معنای آن چه بوده؟

۵. معنای آن در زمان حاضر چیست؟

سؤالات ۱ تا ۳ مشابه رویکردهای معمول برای راستی‌آزمایی هستند و به تعیین نوع تصویر (عکس، ویدیو و غیره)، آنچه که به تصویر می‌کشد و اینکه چه کسی آن را ساخته است، مربوط می‌شود. اما سؤالات ۴ و ۵ ما را به سمت دیگری سوق می‌دهند. این سؤالات نه‌تنها آنچه تصویر نشان می‌دهد، بلکه هرگونه معنایی که به کمک تصاویر تولید می‌شود از جمله معنایی که از طریق شناسایی نادرست تصویر ایجاد می‌شود- را نیز در بر می‌گیرد. کنار هم گذاشتن پرسش‌های ۴ و ۵ به ما کمک می‌کند بر ماهیت متغیر معنای تصاویر تمرکز کنیم و همچنین بر این نکته که معانی‌ای که از طریق استفاده‌ی مجدد به تصاویر نسبت داده می‌شوند به خودی خود می‌توانند اهمیت داشته باشند. بنابراین، این پرسش‌ها فقط به چگونگی استفاده از تصاویر در یک بستر و زمینه‌ی جدید و برداشت نادرستی که از این استفاده‌ی جدید ناشی می‌شود نمی‌پردازند، بلکه تأثیرات این شناسایی‌های نادرست را نیز مد نظر قرار می‌دهند. این رویکرد دیگر تنها به صحت‌سنجی تصاویر محدود نمی‌شود، بلکه بیشتر به تجزیه و تحلیل تصاویر به شیوه‌ای شباهت دارد که در حوزه‌هایی مانند تاریخ هنر و تئوری عکاسی صورت می‌گیرد.

زمانی که مشغول توسعه و اجرای اولیه‌ی این طرح با کمک روزنامه‌نگاران بودیم بارها از آن‌ها می‌شنیدیم که می‌گفتند تابه حال به تصاویر با چنین جزئیاتی فکر نکرده‌اند. بسیاری گفتند که این چارچوب به آن‌ها کمک کرد تا تشخیص دهند که تصاویر اشکال پیچیده‌ای از ارتباط هستند و بررسی و درک معنای آن‌ها نیاز به یک روش نظام‌مند و روشن دارد.

بیشتر مواقع برای به دست آوردن درکی جامع از آنچه که در تصاویر می‌گذرد نیازی نیست به هر ۲۰ سؤال پاسخ دهید. سؤال‌ها به‌گونه‌ای طراحی شده‌اند که در صورت نیاز به منبع لازم برای حل مشکل بررسی تصاویر دسترسی داشته باشید. از نظر ما این سؤال‌ها خاصه هنگام برخورد با تصاویر و ویدئوهای پیچیده‌ی خبری که پرمخاطب هستند و مورد توجه و بررسی دقیق رسانه‌ها قرار گرفته‌اند، مفید هستند. برای اینکه کارکرد این روش را در عمل به شما نشان دهیم، در زیر سه مطالعه‌ی موردی مربوط به بریتانیا و ایالات متحده آورده شده است.

مطالعه‌ی موردی ۱: نقطه‌ی شکست، ژوئن ۲۰۱۶

این تصویر چیست؟

تصویر «نقطه‌ی شکست» درواقع پوستری بود که حزب استقلال بریتانیا (یوکیپ) در طول همه‌پرسی اتحادیه‌ی اروپا در سال ۲۰۱۶ به‌عنوان بخشی از کمپین خود استفاده کرد. در این پوستر از عکسی استفاده شده بود که توسط جف میچل، عکاس خبری، در اکتبر ۲۰۱۵ و با تمرکز بر بحران پناهندگان گرفته شده بود.

تصویر چه چیزی را نشان می‌دهد؟

صف طویلی از پناهجویان سوری و افغان که توسط پلیس اسلوونی از مرز کرواسی و اسلوونی به سمت کمپ آوارگان برژیتسه اسکورت می‌شوند. پوستر از یک نسخه‌ی برش‌خورده استفاده کرده و متن «نقطه‌ی شکست: اتحادیه‌ی اروپا همه‌ی ما را ناامید کرده است» و «باید اتحادیه‌ی اروپا را رها کنیم و کنترل مرزهای خود را پس بگیریم» به آن اضافه شده است. از آنجا که به نظر می‌رسد پناهندگان به‌طور دسته‌جمعی به سمت بیننده حرکت می‌کنند، تصویر تأثیر بصری قوی‌ای ایجاد می‌کند.

چه کسی آن را ساخته است؟

شرکت تبلیغاتی فمیلی اَدورتایزینگ ال‌تی‌دی. مستقر در ادینبرو که توسط حزب یوکیپ (UKIP) [توضیح مترجم فارسی: حزب استقلال پادشاهی متحد، از احزاب سیاسی دست راستی بریتانیا] برای تبلیغات کمپین برگزیت آن‌ها انتخاب شده بود.

معنی این تصویر چه بود؟

حزب یوکیپ سعی نکرده بود تصویر را چیزی غیر از آنچه در واقعیت بود نشان بدهد، اما با اضافه کردن شعارها، لایه‌های دیگری از معنا به آن افزوده بود. با سوء استفاده از احساسات ضدمهاجر و نژادپرستانه‌ی موجود، هدف این عکس ایجاد ترس بیشتر از مهاجران و پناهندگان بر اساس ادعاهای بی‌اساس و کنایات غیرمستقیم در مورد سیاست‌های مرزی اتحادیه‌ی اروپا بود.

معنای این تصویر چیست؟

در نوامبر ۲۰۱۹ و در آستانه‌ی انتخابات عمومی بریتانیا، کمپین خروج از اتحادیه‌ی اروپا، Leave.EU، از نسخه‌ی به‌شدت برش‌خورده‌ای از عکس برای ارسال محتوای ضدمهاجرتی در توئیتر استفاده کرد که به‌وضوح یادآور پوستر سال ۲۰۱۶ یوکیپ بود و به آن ارجاع می‌داد.

پرسیدن چه سؤالات دیگری می‌تواند مفید باشد؟

عامل یک مقام رسمی است یا غیررسمی؟ یوکیپ، عامل اصلی در ایجاد و انتشار این تصویر، یک حزب سیاسی است و بنابراین، از آن نوع عواملی که اغلب با اطلاعات نادرست و دروغ‌پراکنی‌ها در ارتباط هستند محسوب نمی‌شود.

آیا تصویر با تصاویر دیگری ارتباط یا شباهت دارد؟

برخی این پوستر را با تبلیغات حزب نازی مقایسه کرده‌اند. این تصویر هم یادآور تصاویر ضدمهاجرت قدیمی‌تر و هم تاریخچه‌ی طولانی‌تر استفاده از صف‌ها در پوسترهای سیاسی بریتانیا است، از جمله تصویری که در مه ۲۰۱۶ توسط یوکیپ برای تمرکز بر مهاجرت از اتحادیه‌ی اروپا استفاده شده بود.

سه نکته‌ی کلیدی‌ای که از این بررسی به دست می‌آیند عبارتند از:

- **احزاب سیاسی و سیاستمداران می‌توانند در انتشار اطلاعات نادرست نقش داشته باشند.**
- **اطلاعات نادرست همیشه الزاما به معنای استفاده از تصاویر جعلی یا شناسایی نادرست تصاویر نیست. گاهی می‌توان از تصاویر برای پشتیبانی از پیامی استفاده کرد که تصور نادرستی از وضعیت و چشم‌انداز در مقیاسی گسترده‌تر ایجاد می‌کند.**
- **در مورد برخی اطلاعات نادرست، صرف درستی‌سنجی آن‌ها کفایت نمی‌کند، بلکه باید به بررسی انتقادی این نکته پرداخت که چگونه از تصاویر واقعی برای دستکاری احساسات عمومی استفاده می‌شود، این تصاویر چه می‌کنند و چه معنایی دارند.**

نمونه‌هایی از پوشش خبری این مورد در رسانه‌ها:

گاردین: پوستر ضدمهاجر نایجل فراژ به پلیس گزارش شده است

الجزیره: برگزیت: پوستر «غیر اخلاقی» ضد مهاجرت یوکیپ

ایندیپندنت: نایجل فاراژ متهم به استفاده از تبلیغات به سبک حزب نازی هنگام رونمایی از پوستر و سررسیدن طرفداران حزب رقیب

مطالعه‌ی موردی ۲: عکس پل وست‌مینیستر، مارس ۲۰۱۷

این تصویر چیست؟

عکس از حساب کاربری‌ای در توئیتر که ظاهرا متعلق به مردی سفیدپوست اهل تگزاس است توئیت شده و توجه بسیاری را در رسانه‌های اجتماعی به خود جلب کرد. بعدها مشخص شد که این حساب توسط آژانس تحقیقات اینترنتی روسیه اداره می‌شود و برای انتشار اطلاعات نادرست و دروغ‌پراکنی از آن استفاده می‌شود. این توئیت عکسی از وضعیت پس از حمله‌ی تروریستی پل وست‌مینستر در لندن (۲۲ مارس ۲۰۱۷) را به تصویر می‌کشید.

عکس چه چیزی را نشان می‌دهد؟

یک زن مسلمان در حال عبور از کنار گروهی از مردم و یک نفر که در این حمله‌ی تروریستی مجروح شده و روی زمین افتاده است. متن توئیت دارای مفاهیم ضمنی اسلام‌هراسانه است و ادعا می‌کند که این زن عمدا مجروح را نادیده می‌گیرد. یک هشتگ آشکارا ضد اسلامی نیز در توئیت وجود دارد.

چه کسی آن را ساخته است؟

کارمند آژانس تحقیقات اینترنت که حساب توئیتر SouthLoneStar@ را اداره می‌کرد، هرچند در زمان انتشار توئیت مشخص نبود که یک حساب متعلق به آژانس تحقیقات اینترنت روسیه است. خود عکس توسط عکاس مطبوعاتی، جیمی لوریمن گرفته شده است.

معنی عکس چه بود؟

در مارس۲۰۱۷، به نظر می‌رسید که این توئیتی از یک کاربر راست‌گرای تگزاسی در توئیتر است که عکس را اینگونه تفسیر کرده که این زن مسلمان به فرد مجروح اهمیتی نمی‌دهد و معنای ضمنی آن این بود که عکس این زن به حقیقت بزرگ‌تری در مورد مسلمانان اشاره دارد.

معنای عکس چیست؟

تا به امروز، این توئیت شاهدی بر انتشار عمدی اطلاعات نادرست اسلام‌هراسانه توسط آژانس تحقیقات اینترنتی پس از یک حمله‌ی تروریستی است.

پرسیدن چه سؤالات دیگری می‌تواند مفید باشد؟

توئیت چه واکنش‌ها و پاسخ‌هایی دریافت کرد؟ این توئیت واکنش قابل‌توجهی از رسانه‌های جریان اصلی دریافت کرد. بسیاری از روزنامه‌های بریتانیایی (بعضا بیش از یک بار) درباره‌ی آن مطالبی منتشر کردند. اگرچه بیشتر این مطالب توئیت SouthLoneStar@ را محکوم می‌کردند، درعین‌حال باعث شدند محتوای توئیت از محدوده‌ی شبکه‌های اجتماعی خارج شود و در اختیار طیف گسترده‌تری از مخاطبان قرار بگیرد. پس از انتشار تصویر، زن حاضر در عکس در صحبت‌هایی گفت که از دیدن عکسش بسیار ناراحت و نگران شده: «نه‌تنها از دیدن عواقب یک حمله‌ی تروریستی تکان‌دهنده و فلج‌کننده ویران شده بودم، بلکه مجبور شدم با شوک ناشی از پخش شدن عکسم در رسانه‌های اجتماعی توسط کسانی که نمی‌توانند از ظاهرم فراتر بروند و بر اساس نفرت و بیگانه‌هراسی قضاوتم می‌کنند نیز روبرو شوم.»

آیا تصویر به تصاویر دیگری شباهت یا ارتباط دارد؟

عکس منتشرشده یکی از ۷ عکسی بود که از این زن گرفته شده بود و در باقی عکس‌ها به وضوح دیده می‌شد که زن ناراحت و نگران است اما تعداد کمی از نشریات به این واقعیت توجه نشان دادند.

عکس به چه میزان و تا چه مدت در حال پخش شدن بود؟

افزایش توجه رسانه‌های جریان اصلی به این عکس به معنای آن بود که عکس به‌سرعت پخش می‌شود. بااین‌حال، در عرض چند روز گردش و انتشار عکس به‌طرز چشمگیری کاهش پیدا کرد. در نوامبر ۲۰۱۷ و زمانی که کاشف به عمل آمد حساب کاربری SouthLoneStar@ توسط آژانس اطلاعات اینترنت روسیه اداره می‌شود عکس دوباره به گردش افتاد اما این گردش در رسانه‌های اصلی در مقایسه با ماه مارس بسیار ناچیزتر بود.

سه نکته‌ی کلیدی‌ای که از این بررسی به دست می‌آیند:

- **اطلاعات نادرست بصری همیشه کاملا نادرست نیستند و می‌توانند شامل عناصری مبتنی بر حقیقت باشند. در اینجا عکس مورد نظر واقعی است، اما زمینه و بستر آن دستکاری شده و دروغین است، و معنای آن متکی بر این واقعیت است که خواننده/بیننده نمی‌داند آن زن واقعا در آن لحظه به چه چیزی فکر می‌کرده است.**
- **روزنامه‌نگاران باید در مورد جلب توجه بیشتر از طریق گزارش دادن (حتی با نیت مثبت) درباره‌ی چنین اطلاعات نادرستی که احساسات عمومی را تحریک می‌کنند و بحث‌انگیز و بالقوه مضر هستند هشیار و مراقب باشند.**
- **تصحیح اخبار مبتنی بر اطلاعات نادرست و حصول اطمینان از انتشار تصویر واقعی رویدادها باید بیشتر مورد توجه قرار گیرد. پوشش محدود در ماه نوامبر به این معنی است که برخی از خوانندگان ممکن است متوجه نشده باشند که این توئیت درواقع اطلاعات نادرستی بوده که توسط روسیه پراکنده شده است.**

نمونه‌هایی از پوشش خبری این مورد در رسانه‌ها:

میرِر: ساختن فرضیات نگران‌کننده درباره‌ی «زنی باحجاب که از کنار مرد مجروح می‌گذرد» توسط مردم

دِیلی مِیل: «هیولای واقعی کیست؟» انتقادها در فضای مجازی به اوباش اینترنتی‌ای که به زن مسلمان «بی‌تفاوت», که از کنار مرد مجروح حمله‌ی تروریستی می‌گذرد حمله کردند

گاردین: نماینده‌ی بریتانیا از توئیتر خواست توئیت‌های «کارخانه‌ی اوباش اینترنتی» روسیه را منتشر کند

مطالعه‌ی موردی ۳: درگیری در بنای یادبود لینکلن

این تصویر چیست؟

ویدئویی از گروهی از دانش‌آموزان دبیرستان کاتولیک کاوینگتون که در راهپیمایی «برای زندگی»

شرکت کردند و یک مرد بومی به نام ناتان فیلیپس که دیگر بومیان آمریکا را در راهپیمایی مردمان بومی همراهی می‌کرد.

تصویر چه چیزی را نشان می‌دهد؟

رویارویی بین یکی از دانش‌آموزان دبیرستان کاتولیک کاوینگتون و فیلیپس. دو گروه از تظاهرات‌کنندگان در پلازا به هم رسیدند و گروه بزرگی از دانشجویان کاوینگتون که کلاه MAGA بر سر داشتند، ظاهرا در مقابل فیلیپس صف‌آرایی کردند. این تصویر مرد بومی‌ای را نشان می‌دهد که به‌تنهایی در برابر صف دانش‌آموزان قلدر راست آلترناتیو قد علم کرده است.

چه کسی آن را ساخته است؟

این ویدئو اولین بار توسط یکی از شرکت‌کنندگان در راه‌پیمایی مردمان بومی در اینستاگرام به اشتراک گذاشته شد و تقریبا ۲۰۰ هزار بازدید داشت. ساعاتی بعد، ویدئو در توئیتر آپلود شد و قبل از حذف توسط حساب اصلی، ۲.۵ میلیون بار دیده شد. سپس ویدئو در سایت‌های مختلف رسانه‌های اجتماعی بازنشر شد و متعاقبا توجه رسانه‌های اصلی را نیز به خود جلب کرد. در عرض ۲۴ ساعت، چندین مقاله در مورد این ویدئو منتشر شد.

معنی آن چه بود؟

روایت اولیه که در فضای مجازی پخش شد، ویدئو را به عنوان یک رویارویی مستقیم بین فیلیپس و دانش‌آموزانی نشان داد که عمدا فیلیپس را مسخره می‌کنند و سربه‌سرش می‌گذارند.

معنای آن چیست؟

ویدئوی طولانی‌تر دیگری که چند روز پس از ویدئوی اول منتشر شد، تصویر پیچیده‌تری را ترسیم کرد. گروهی از بنی‌اسراییلی‌های عبری سیاه‌پوست نیز در بنای یادبود حضور داشتند که مشغول متلک‌پرانی به رهگذرها، از جمله دانش‌آموزان کاوینگتون و شرکت‌کنندگان در راه‌پیمایی مردمان بومی بودند. این باعث یک درگیری شدید بین هر سه گروه شد و ظاهرا فیلیپس قصد آرام کردن طرفین درگیری را داشته است. ویدئوی اول از همین صحنه شروع می‌شود.

پرسیدن چه سؤال‌های دیگری می‌تواند مفید باشد؟

چه اطلاعات زمینه‌ای دیگری برای درک درست ویدئو نیاز دارید؟

بدون دیدن ویدئوی طولانی‌تر و فهمیدن اینکه عبری‌های سیاه‌پوست هم در مکان حضور داشتند و فعالانه به درگیری دامن می‌زدند، درواقع زمینه‌ی اصلی ماجرا از دست می‌رود. درحالیکه دانش‌آموزان در حال بر زبان راندن سخنان نژادگرایانه دیده می‌شوند، آنچه درواقع منجر به این درگیری شده چیزی بیش از صف‌آرایی دانش‌آموزان قلدر در برابر یک مرد بومی تنها است.

ویدئو در کدام شبکه‌های اجتماعی به اشتراک گذاشته شد؟

ویدئوی اصلی توسط یکی از شرکت‌کنندگان در راه‌پیمایی مردمان بومی در اینستاگرام به اشتراک گذاشته شده بود که توجه نسبتا محدودی را جلب کرد. زمانی که ویدئو متعاقبا توسط سایر کاربران در توئیتر و یوتیوب به اشتراک گذاشته شد آگاهی در مورد آن به‌شدت تقویت شده و توجه رسانه‌های جریان اصلی نیز به آن جلب شد. بنابراین، موج توجه اصلی نه از اشتراک‌گذاری اولیه، بلکه از این اشتراک‌گذاری‌هایی که متعاقبا صورت گرفت ناشی شده بود.

سه نکته‌ی کلیدی‌ای که از این بررسی به دست می‌آیند:

- **زمانی که تصاویری با محتوایی چنین برانگیزاننده و احساسی در فضای مجازی پخش می‌شوند، زمینه‌ی وقوع آن‌ها می‌تواند به راحتی فراموش شده و نادیده گرفته شود و روایت واکنشی‌ای که در فضای مجازی شکل گرفته به سرعت تبدیل به روایت غالب شود.**

- **با نگاه به گذشته، برخی از روزنامه‌نگاران استدلال کردند که مقاله‌های اولیه به جنجال دامن زده و روایت نادرست را بیشتر در مرکز توجه قرار دادند. این نشان می‌دهد که بدون بررسی‌های مناسب، رسانه‌های جریان اصلی می‌توانند ناخواسته به انتشار اطلاعات نادرست ادامه دهند.**
- **سرعت پخش آنلاین ویدئو به این معنی بود که بسیاری از رسانه‌های جریان اصلی روایتی را که در**

رسانه‌های اجتماعی منتشر شده بود «باور کردند» و بیشتر تحقیق نکردند. پس از مشخص شدن ابعاد بیشتر ماجرا، بسیاری از سایت‌های خبری مجبور به پس گرفتن یا تصحیح مقاله‌های خود شدند و از برخی از آن‌ها نیز شکایت شد.

نمونه‌هایی از پوشش خبری این مورد در رسانه‌ها:

یونی‌لند: دوره کردن و مسخره کردن کهنه‌سرباز جنگ ویتنام و بومی آمریکا توسط نوجوان‌های کلاه MAGA به سر

گاردین: اعتراض‌ها پس از آنکه دانش‌آموزان کنتاکی با کلاه MAGA کهنه‌سرباز بومی آمریکا را مسخره کردند

یواس‌ای تودِی: ویدئوی کامل‌تر جزئیات جدیدی از رویارویی دانش‌آموزان کاتولیک کاوینگتون و مرد بومی سالخورده را روشن کرده است

نتیجه‌گیری

بسیاری از آنچه در رسانه‌های اجتماعی به اشتراک گذاشته می‌شود، محتوای تصویری است. روزنامه‌نگاران باید به توانایی بررسی انتقادی و ارزیابی تصاویر با هدف پی بردن به محتوا و مقاصد مهمی که در آن‌ها مستتر است مجهز شوند. سرعت انتشار اطلاعات نادرست بصری، نیاز روزنامه‌نگاران به رعایت احتیاط و اطمینان از بررسی کامل داستان‌های مرتبط با تصویر قبل از انتشار آن را بیشتر برجسته می‌کند. ۲۰ سؤال برای بررسی تصاویر رسانه‌های اجتماعی ابزار دیگری است که روزنامه‌نگاران می‌توانند هنگام بررسی تصاویر از آن استفاده کنند، به‌ویژه زمانی که داستان عمدتا بر روی محتوای بصری متمرکز است. استفاده از هر ۲۰ سؤال برای درک تمام تصاویر ضروری نیست، اما ۵ سؤال اول می‌توانند نقطه‌ی شروع بسیار خوب و قدرتمندی باشند. هدف از طرح این ۵ سؤال، که باید با کمک مهارت‌های پایه‌ی درستی‌سنجی پاسخ داده شوند، تهیه‌ی گزارش‌های دقیق‌تر و عمیق‌تر است.

ضمیمه

در زیر فهرست کاملی از سؤالات طرح ۲۰ پرسش، شامل ۱۴ پرسش کوتاه که به‌طور خاص بر اطلاعات نادرست و دروغ‌پراکنی متمرکز است، ارائه شده است. همانطور که در این فصل اشاره کردیم، بهتر است بررسی هر تصویر را با ۵ سؤال اول شروع کنیم. سؤالات کوتاه به عامل انتشار تصویر، پیام آن و کسی می‌پردازد که اطلاعات نادرست را تفسیر کرده است:

عامل - چه کسی تصویر را ایجاد و توزیع کرده و انگیزه او چه بوده است؟

پیام - تصویر چه شکلی گرفته است و چه ویژگی‌هایی دارد؟

مفسر - پیام چگونه تفسیر شده و چه اقداماتی در خصوص آن انجام شده است؟

1. **What is it?**
2. How was it produced?
3. For what purpose was it made?
    a. A - Financial, Political, Social, Psychological or Other?
    b. M - Who or what was the message's intended target?
4. Who were the intended audience?
5. **What does it show?**
6. **What *does* it mean?**
    a. M - Is it imposter content i.e. posing as an official source?
    b. M - How accurate is the message?
7. **What *did* it mean?**
    a. A - Is there an intent to harm and or mislead?
8. What text accompanied it and framed its meaning?
    a. M - Is it accurate, misleading, manipulated, or fabricated?
9. What contextual information do you need to know?
    a. M - Is the message legal?
10. Is it similar to or related to other images?
11. **Who made it?**
    a. A - Is the actor official or unofficial?
    b. A - Level of organisation: none, loose, tight, or networked?
12. Was it shared on social media by the person who made it?
    a. A - Was it shared by a human, cyborg, or a bot?
    b. A - Is there an intent to harm and or mislead?
13. If not, who shared it on social media?
14. Was it originally made for social media?
15. If not, where did it originate?
16. Where was it shared on social media?
    a. I - Interpreted differently by different people? If so, how?
17. How widely and for how long was it circulated?
    a. M - Was it long-term, short-term, or event-led?
18. What responses did it receive?
    a. I - What action was taken? Was the message reproduced?
19. Who else used it on social media?
20. Does social media sharing raise ethical concerns?

منابعی که الهام‌بخش تولید این طرح بوده‌اند:

The «Interrogating the work of Art» diagram (Figure 2.4, p.39), in (5 ,2014th Edition), Pointon, M. **History of Art: A Student's Handbook**, London and New York: Routledge.

«Questions to ask about each element of an example of information disorder» (Figure 7, p. 28), in (2017), Wardle, C. and Derakshan, H., **Information Disorder: Toward an interdisciplinary framework for research and policy making.** Council of Europe report DGI(09(2017.

۶. در مورد دیپ‌فیک‌ها و سایر فناوری‌های نوظهور دستکاری تصاویر چه می‌دانیم

نوشته‌ی: سم گرگوری

سم گرگوری مدیر برنامه‌ها در ویتنس (www.witness.org) است و به مردم کمک می‌کند از تکنولوژی و ویدئوها برای دفاع از حقوق بشر استفاده کنند. او که یک فناور (Technologist) و مدافع حقوق بشر است برای فعالیت‌هایش جوایزی برده و در زمینه‌ی اشکال جدید دروغ‌پراکنی و انتشار اطلاعات نادرست با استفاده از هوش مصنوعی تخصص دارد و در زمینه‌ی فرصت‌ها و تهدیدهای جدیدی که این فناوری‌ها برای کنشگران و روزنامه‌نگاران به همراه دارند، کار می‌کند. او همچنین یکی از رؤسای کارگروه هوش مصنوعی و رسانه در کنسرسیوم مشارکت در هوش مصنوعی است.

در تابستان سال ۲۰۱۸، پروفسور سی‌وی لیی، محقق برجسته‌ی دیپ‌فیک از دانشگاه آلبانی، مقاله‌ای منتشر کرده بود که در آن نشان می‌داد سرعت پلک زدن شخصیت‌های ویدئویی دیپ‌فیک با سرعت پلک زدن انسان متفاوت است. این ادعا به‌زودی توسط فست کامپنی، سی‌بی‌اس نیوز، گیزمودو، نیو ساینتیست و دیگران پوشش داده شد، و باعث شد بسیاری فکر کنند که دیگر روشی قوی برای شناسایی دیپ‌فیک‌ها در اختیار دارند.

بااین‌حال، هنوز چند هفته از انتشار مقاله نگذشته، این محقق ویدئوهایی دریافت کرد حاوی شخصیت‌های دیپ‌فیکی که درست مثل یک انسان پلک می‌زدند. در حال حاضر نکته‌ای که پروفسور لیی به آن اشاره کرده بود دیگر نه دقیق است و نه مفید. این نکته در آن لحظه پاشنه‌ی آشیل الگوریتم ایجاد دیپ‌فیک بود و در مجموعه داده‌ی آموزشی‌ای ریشه داشت که برای ساخت الگوریتم مورد استفاده قرار گرفته بود. اما در عرض چند ماه این ایراد دیگر مصداق نداشت.

این مثال یک حقیقت کلیدی را در مورد تشخیص و راستی‌آزمایی دیپ‌فیک‌ها نشان می‌دهد: رویکردهای فنی تا زمانی مفید هستند که تکنیک‌های رسانه‌ی مصنوعی ناگزیر با آنها سازگار شوند. یک سیستم عالی و بی‌نقص برای تشخیص دیپ‌فیک هرگز وجود نخواهد داشت.

پس خبرنگاران چگونه باید دیپ‌فیک‌ها و سایر اشکال رسانه‌های مصنوعی را شناسایی کنند؟

اولین قدم این است که ماهیت موش‌وگربه‌ای این کار را درک کنید و از چگونگی پیشرفت فناوری آگاه باشید. در دومین قدم روزنامه‌نگاران باید با تکنیک‌های پایه و ابزارهای راستی‌آزمایی آشنا شوند و آن‌ها را به کار ببندند و ابزار لازم را داشته باشند تا بتوانند بررسی کنند یک ویدئوی خاص واقعی است، با اهداف سوء دستکاری شده و یا اصولا ساختگی و مصنوعی است. روش‌های راستی‌آزمایی تصاویر و ویدئوها که در جلد اول کتابچه‌ی راهنمای راستی‌آزمایی و همچنین در منابع فرست درفت مربوط به راستی‌آزمایی بصری به آن‌ها اشاره شده، کماکان کاربردی و مفید هستند. درنهایت، روزنامه‌نگاران باید به این نکته توجه داشته باشند که ادعای اینکه محتوایی در واقع دیپ‌فیک است در محیط اطلاعاتی کنونی ما تبدیل به امر بسیار رایجی شده است. و این بدان معناست که توانایی تأیید صحت یک عکس یا ویدئو به همان اندازه مهم است که بتوانیم ثابت کنیم که آن عکس یا ویدئو دستکاری شده است.

این فصل در مورد این رویکردهای اصلی برای تأیید دیپ‌فیک‌ها توضیح می‌دهد، اما پیش از هر چیز مهم است که درکی پایه از دیپ‌فیک‌ها و رسانه‌های مصنوعی داشته باشید.

دیپ‌فیک و رسانه‌ی مصنوعی چیست؟

دیپ‌فیک یا همان جعل عمیق شکل جدیدی از دستکاری سمعی و بصری است که به افراد امکان می‌دهد شبیه‌سازی‌هایی بسیار نزدیک به چهره، صدا یا اعمال واقعی اشخاص ایجاد کنند. به کمک این تکنولوژی می‌توان تصاویری از گفته‌ها و اعمالی ساخت که هرگز در واقعیت گفته نشده و اتفاق نیافتاده‌اند. ساخت محتوای دیپ‌فیک روزبه‌روز آسان‌تر می‌شود و به تصاویر منبع کمتری نیاز دارد و بیش از پیش برای کسب سود ساخته و خرید و فروش می‌شود. در حال حاضر، دیپ‌فیک‌ها بیشترین تأثیر را بر زنان می‌گذارند، زیرا از آن‌ها برای ایجاد تصاویر و ویدئوهای جنسی با چهره‌ی یک فرد خاص بدون اطلاع و رضایت او استفاده می‌شود. اما این نگرانی وجود دارد که دیپ‌فیک‌ها تأثیر گسترده‌تری در سراسر جامعه و در فرآیندهای جمع‌آوری و راستی‌آزمایی اخبار نیز داشته باشند. دیپ‌فیک تنها یکی از روش‌ها در خانواده‌ی بزرگ‌تر تکنیک‌های مبتنی بر هوش مصنوعی برای تولید رسانه‌های مصنوعی

است. این مجموعه از ابزارها و تکنیک‌ها امکان ایجاد شبیه‌سازی‌های بسیار نزدیک به واقعیت از کارها و گفته‌هایی که در واقعیت انجام و گفته نشده‌اند، خلق افراد/اشیایی که هرگز وجود نداشته‌اند یا رویدادهایی که هرگز اتفاق نیفتاده‌اند را فراهم می‌کند.

در حال حاضر، تکنولوژی‌های رسانه‌ی مصنوعی امکان دستکاری‌های زیر را فراهم می‌کنند:

- **حذف یا افزودن شیئی خاص به یک ویدئو**
- **تغییر شرایط و پس‌زمینه‌ی ویدئو. به‌عنوان مثال، تغییر شرایط آب‌وهوا و یا تبدیل فصلی که ویدئو در آن گرفته شده از زمستان به تابستان**
- **شبیه‌سازی و کنترل یک نمایش شبیه به واقعیت از حرکت لب‌ها، حالات صورت یا حرکت بدن یک فرد خاص. اگرچه بحث دیپ‌فیک به‌طور کلی روی صورت‌ها متمرکز است، تکنیک‌های مشابهی برای حرکت تمام بدن یا قسمت‌های خاصی از صورت نیز به کار می‌رود.**
- **ساخت تقلیدی شبیه به واقعیت از صدای یک فرد خاص**
- **تغییر صدای موجود با استفاده از ,پوست صدا (Skin Voice)، یک جنسیت متفاوت و یا صدای یک شخص خاص**
- **ایجاد یک عکس واقعی کاملا جعلی از شخصی که وجود ندارد. همین تکنیک همچنین می‌تواند با مشکلات کمتری برای ساختن چیزهایی مثل یک همبرگر، گربه و سایر موارد تقلبی نیز استفاده شود.**
- **انتقال یک حالت چهره‌ی واقعی از شخصی به شخص دیگر یا همان دیپ‌فیک.**

این تکنیک‌ها عمدتا، اما نه منحصرا، بر نوعی از هوش مصنوعی به نام یادگیری عمیق و شبکه‌های مولد رقابتی، GANها (Generated Adversarial Networks) متکی هستند.

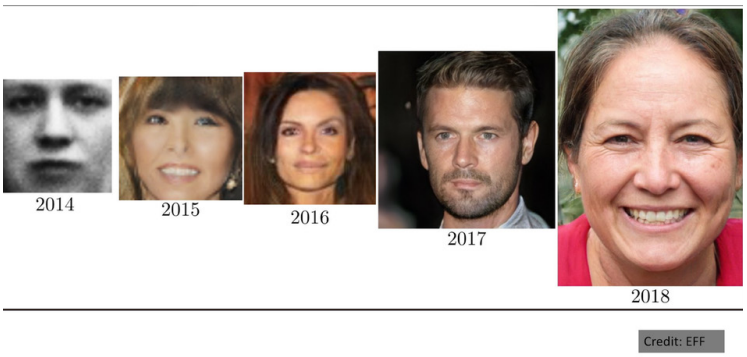
برای تولید یک محتوای رسانه‌ی مصنوعی، باید کار خود را با جمع‌آوری تصاویر یا ویدئوهای منبع از شخص یا موردی که می‌خواهید جعل کنید، شروع کنید. GAN کار ساخت محتوای جعلی مورد نظر شما را -چه این محتوا شبیه‌سازی چهره‌ی یک شخص واقعی باشد و چه تعویض دو چهره با هم- با استفاده از دو شبکه انجام می‌دهد. یک شبکه بازآفرینی‌های قابل قبولی از تصاویر منبع ایجاد می‌کند، در حالیکه شبکه‌ی دوم تلاش می‌کند این جعل‌سازی‌ها را شناسایی کند. سپس این داده‌های شناسایی

به شبکه‌ای که کار جعل را انجام می‌دهد بازخورد داده می‌شود و آن را قادر می‌سازد کارکرد خود را بهبود ببخشد.

تا اواخر سال ۲۰۱۹، بسیاری از این تکنیک‌ها -به‌ویژه تکنیک‌های ساخت دیپ‌فیک- نیازمند قدرت محاسباتی قابل‌توجه، درک نحوه‌ی تنظیم مدل و نمونه، و استفاده از گرافیک رایانه‌ای (سی‌جی‌آی) برای ویرایش تصاویر ساخته‌شده و بهبود نتایج بود. بااین‌حال و علی‌رغم محدودیت‌های فعلی، انسان‌ها در حال حاضر نیز فریب رسانه‌های شبیه‌سازی را می‌خورند. به‌عنوان مثال، تحقیقات پروژه FaceForensics++ نشان داد که افراد نمی‌توانند اشکال فعلی تغییر حرکت لب را که برای تطبیق دهان شخص با صدای ضبط‌شده‌ی جدید استفاده می‌شود، به‌طور قابل اعتماد تشخیص دهند. این بدان معناست که انسان‌ها ذاتا به توانایی تشخیص دستکاری رسانه‌های مصنوعی مجهز نیستند.

همچنین لازم به ذکر است که تکنولوژی ترکیب و همانندسازی صوتی سریع‌تر از حد انتظار در حال پیشرفت است و به‌صورت تجاری نیز در دسترس قرار دارد. به‌عنوان مثال، Google Cloud Text-to-Speech API شما را قادر می‌سازد تا یک متن را با صدای واقعی انسان به شکل محتوای صوتی درآورید. تحقیقات اخیر همچنین بر امکان انجام ویرایش‌های ترکیبی متن به ویدئو/صوت در مصاحبه‌ها متمرکز شده است.

به‌علاوه، تمام شواهد فنی و تجاری‌سازی حاکی از آن است که ساخت رسانه‌های مصنوعی متقاعدکننده در آینده آسان‌تر و کم‌هزینه‌تر خواهد شد. به‌عنوان مثال، تصویر زیر نشان می‌دهد که فناوری تولید چهره با چه سرعتی پیشرفت کرده است.



به دلیل ماهیت موش‌وگربه‌ی این شبکه‌ها، به مرور زمان و با دریافت بازخورد درباره‌ی جعل‌های موفق و موارد شناسایی موفقیت‌آمیز رسانه‌های مصنوعی کارکرد آن‌ها نیز بهبود پیدا می‌کند. همین امر احتیاط شدید در مورد اثربخشی روش‌های تشخیص این رسانه‌های مصنوعی را ایجاب می‌کند.

چشم‌انداز دیپ‌فیک و رسانه‌های مصنوعی در زمان حاضر

دیپ‌فیک‌ها و رسانه‌های مصنوعی (هنوز) در خارج از حیطه‌ی تصاویر جنسی ساختگی بدون رضایت افراد، چندان رایج و مورد استفاده نیستند. گزارش دیپ‌تِریس لب در مورد شیوع این نوع محتوا در سپتامبر ۲۰۱۹ نشان می‌دهد که بیش از ۹۵درصد دیپ‌فیک‌ها از این نوع بوده‌اند و قربانیان آن‌ها شامل افراد مشهور، بازیگران زن فیلم‌های پورن یا افراد عادی می‌شود. به‌علاوه، اخیرا تمایل برای به چالش کشیدن محتوای واقعی و شناسایی محتوا به‌عنوان دیپ‌فیک نیز در میان افراد افزایش پیدا کرده است.

در کارگاه‌هایی که توسط ویتنس برگزار شده است، مسیر تهدیدهای بالقوه را با حضور طیفی از شرکت‌کنندگان جامعه‌ی مدنی، از جمله رسانه‌های مردمی، روزنامه‌نگاران حرفه‌ای و راستی‌آزماها، و همچنین محققان اطلاعات نادرست و دروغ‌پراکنی و متخصصان اطلاعات منبع‌باز (OSINT) بررسی کردیم. حوزه‌هایی که در آن اشکال جدید دستکاری ممکن است تهدیدهای موجود را گسترش دهند، تهدیدهای جدیدی را معرفی کنند، تهدیدات موجود را تغییر دهند یا تهدیدات دیگر را تقویت کنند، اولویت‌بندی کردیم. همچنین تهدیدهایی را که متوجه روزنامه‌نگاران، راستی‌آزماها و محققین منبع‌باز است و حملات احتمالی به فرآیندهای آن‌ها را نیز شناسایی کردیم. برجسته‌سازی چالش‌هایی که حول ادعاهایی از جنس «این محتوا دیپ‌فیک است» به‌عنوان خویشاوند ادعاهای دیگری مانند «این اخبار جعلی است» وجود دارد نیز از جمله دیگر موضوعاتی بود که به آن‌ها پرداختیم.

همکاران ما در همه‌ی زمینه‌ها، به اهمیت مشاهده‌ی دیپ‌فیک در چارچوب رویکردهای موجود برای صحت‌سنجی و راستی‌آزمایی اشاره کردند. به گفته‌ی آن‌ها دیپ‌فیک‌ها و رسانه‌های مصنوعی در کمپین‌های توطئه‌ای و اطلاعات نادرست موجود ادغام می‌شوند و از تاکتیک‌های (و پاسخ‌های) در حال تکامل در این حوزه استفاده می‌کنند.

این‌ها بعضی از تهدیداتی هستند که همکاران و گروه متخصصان ما به آن‌ها اشاره کرده‌اند:

- اعتبار و شهرت روزنامه‌نگاران و فعالان مدنی با تکیه بر اشکال موجود آزار و اذیت آنلاین و خشونت، که عمدتا زنان و اقلیت‌ها را هدف قرار می‌دهند، مورد حمله قرار خواهد گرفت. پیش از این نیز حملاتی چند با استفاده از ویدئوهای دستکاری‌شده علیه زنان روزنامه‌نگار انجام شده است؛ مانند مورد رعنا ایوب، روزنامه‌نگار برجسته‌ی هندی.
- شخصیت‌های شناخته‌شده در عرصه‌ی عمومی با ویدئوهایی دارای محتوای رابطه‌ی جنسی بدون‌رضایت، خشونت مبتنی بر جنسیت و سایر محتواهایی که با استفاده از افرادی که اصطلاحا «همزاد» آن‌ها نامیده می‌شوند تولید شده، مواجه خواهند شد. سیاستمداران محلی ممکن است به‌ویژه در این حوزه آسیب‌پذیر باشند، زیرا درعین‌حال که تصاویر بسیاری از آن‌ها وجود دارد، ساختارها و نهادهایی که از سیاست‌مداران در سطح ملی دفاع می‌کنند، برای دفاع از آن‌ها در برابر رسانه‌های مصنوعی وجود ندارند. آن‌ها همچنین اغلب منابع کلیدی در پوشش‌های خبری‌ای هستند که از سطح محلی به سطح ملی گسترش پیدا می‌کنند.
- از آنِ خودسازی برندهای شناخته‌شده با ویرایش و تحریف محتوای ویدئوها یا روش‌های دیگری که از طریق آنها ممکن است یک برند خبری، دولتی، شرکتی یا سازمان غیردولتی به‌طور نادرست به یک محتوا متصل شود.
- تلاش برای وارد کردن محتوای دستکاری‌شده‌ی تولید شده توسط یک کاربر در چرخه‌ی اخبار، همراه با تکنیک‌های دیگر مانند هک کردن منبع یا به اشتراک گذاشتن محتوای دستکاری‌شده با خبرنگاران در لحظات کلیدی. به‌طور معمول، هدف وادار کردن خبرنگاران به تبلیغ و تقویت این محتوای نادرست است.
- استفاده از ضعف‌های فرآیند جمع‌آوری اخبار/گزارش‌دهی مانند پخش از راه دور تک دوربینی (همانطور که تیم محتوای تولیدی کاربران رویترز نیز به آن اشاره کرده است) و جمع‌آوری مطالب در زمینه‌های غیرقابل تأیید، مانند مناطق جنگی یا مکان‌های دیگر.
- همان‌طور که تولید دیپ‌فیک‌ها رایج‌تر و تولید آن‌ها در حجم‌های بیشتر ممکن می‌شود، سیلی از مطالب کذب به آژانس‌های راستی‌آزمایی و درستی‌سنجی رسانه‌ای سرازیر خواهد شد؛ مطالبی که این آژانس‌ها باید آن‌ها را تأیید و یا از اعتبار ساقط کنند. این می‌تواند فشار بیش از حدی بر آن‌ها وارد کرده و گیجشان کند.

- **فشار بر سازمان‌های جمع‌آوری و صحت‌سنجی اخبار برای ثابت کردن اینکه خبری درست است و تحریف یا دروغ نیست افزایش پیدا خواهد کرد. صاحبان قدرت این فرصت را به دست خواهند آورد که صحت محتوا را به چالش بکشند و ادعا کنند محتوای خاصی درواقع دیپ‌فیک است.**

نقطه‌ی شروع برای شناسایی دیپ‌فیک‌ها

با توجه به ماهیت بررسی و تحلیل علمی محتوای رسانه و تکنولوژی‌های در حال ظهور دیپ‌فیک، باید بپذیریم که صِرف فقدان شواهد دال بر دستکاری چیزی دلیل قطعی بر اینکه دستکاری‌ای صورت نگرفته نخواهد بود.

لازم است روزنامه‌نگاران و محققان ذهنیتی شامل شک و تردید به‌قاعده و به‌اندازه در مورد عکس‌ها، فیلم‌ها و صداها را در خود ایجاد کنند. آن‌ها باید فرض را بر این بگذارند که با افزایش دانش و ترس از دیپ‌فیک، این اشکال از رسانه‌ها بیشتر به چالش کشیده خواهند شد. همچنین، آشنایی با ابزارهای بررسی و تحلیل محتوای رسانه نیز برای آن‌ها ضروری است.

با در نظر گرفتن این موضوع، هر رویکردی برای تجزیه و تحلیل و شناسایی دیپ‌فیک‌ها و دستکاری به شیوه‌ی تولید رسانه‌های مصنوعی باید شامل موارد زیر باشد:

۱. بررسی محتوا برای پیدا کردن خطاهای از روی بی‌فکری و همچنین اعوجاج‌هایی که نشان از دیپ‌فیک بودن محتوا داشته باشند

۲. به‌کارگیری روش‌های موجود برای تجزیه و تحلیل، بررسی و تأیید صحت ویدئوها

۳. آشنا شدن و استفاده از رویکردهای جدید مبتنی بر هوش مصنوعی و رویکردهای نوظهور بررسی علمی هر زمانی که موجود باشند.

بررسی پرش‌ها یا اعوجاج‌های آشکار

این ساده‌ترین روش شناسایی دیپ‌فیک‌ها و سایر تغییرات رسانه‌ی مصنوعی، به‌ویژه با توجه به ماهیت در حال تکامل این فناوری است. دیپ‌فیک‌ها یا محتوای مصنوعی ضعیف ممکن است شواهدی از خطاهای قابل مشاهده را ارائه دهند. چیزهایی که باید در دیپ‌فیک‌ها جستجو کنید عبارتند از:

- **اعوجاج‌های احتمالی در پیشانی/خط موها و یا حرکت قسمتی از صورت خارج از حوزه‌ی طبیعی حرکت آن قسمت**
- **عدم وجود جزئیات روی دندان‌ها**
- **پوست بیش از حد صاف**
- **پلک نزدن**
- **یک سخنگوی ثابت بدون حرکت واقعی سر یا اشکال دیگر بیان احساسات هنگام صحبت کردن**
- **پرش تصویر هنگامی که فرد رو به دوربین به پهلو می‌چرخد**

در حال حاضر برخی از این اشکالات بیشتر در تجزیه و تحلیل فریم به فریم قابل مشاهده هستند، بنابراین استخراج یک سری فریم برای بررسی جداگانه می‌تواند کمک کند. البته این در خصوص اعوجاج‌هایی که در اثر حرکات جلویی-جانبی ایجاد می‌شوند صدق نمی‌کند؛ اینگونه اعوجاج‌ها در حرکت پیوسته بهتر دیده می‌شوند، بنابراین باید از هر دو روش استفاده کنید.

استفاده از روش‌های موجود دیگر برای صحت‌سنجی ویدئوها

مانند سایر اشکال دستکاری رسانه‌ها و جعل سطحی (از جمله ویدئوهایی که در بستری غیر از بستر و زمینه‌ی واقعی خود مورد استفاده قرار گرفته یا ویرایش شده‌اند) در اینجا نیز باید روش خود را بر شیوه‌های تأییدشده‌ی راستی‌آزمایی مستقر کنید. روش‌های راستی‌آزمایی اطلاعات منبع‌باز (OSINT) هنوز هم معتبر هستند، و فصل‌ها و مطالعات موردی مربوط به صحت‌سنجی تصاویر و ویدئوها در جلد اول کتابچه‌ی راهنمای راستی‌آزمایی می‌تواند نقطه‌ی شروع خوبی باشد. از آنجایی که اکثر دیپ‌فیک‌ها

در حال حاضر به‌طور کامل ساختگی نیستند و با ایجاد تغییرات در یک ویدئوی منبع ساخته می‌شوند، می‌توانید فریم‌هایی از یک ویدیو را انتخاب کرده و با جستجوی معکوس آن‌ها، نسخه‌های احتمالی دیگر ویدئو در فضای مجازی را پیدا کنید. همچنین می‌توانید مناظر و مکان‌های خاص در ویدئو را با نقشه‌های Google Street View مطابقت داده و عدم‌تطابق‌های احتمالی را پیدا کنید.

به همین ترتیب، درک نحوه‌ی به اشتراک گذاری محتوا، و اینکه توسط چه کسی و چگونه به اشتراک گذاشته شده است می‌تواند کمک کند بفهمید آیا می‌توانید به عکس یا ویدئوی خاصی اطمینان کنید یا نه. اصول تعیین منبع، تاریخ، زمان و انگیزه‌ی به‌اشتراک‌گذاری یک محتوا برای تعیین اینکه آیا آن محتوا به رویداد یا شخصی واقعی مربوط می‌شود یا خیر، ضروری است. (برای به دست آوردن دانش پایه‌ی مورد نیازتان در این زمینه می‌توانید از این راهنمای فرست درفت استفاده کنید). و مثل همیشه، لازم است با فرد یا افرادی که در ویدئو نشان داده شده‌اند تماس بگیرید و بخواهید که درباره‌ی آن اظهارنظر کنند و ببینید آیا آن‌ها می‌توانند اطلاعات دقیقی در حمایت یا رد صحت آن ارائه دهند یا خیر.

ابزارهای جدیدی نیز توسط دولت، محققان، پلتفرم‌ها و آزمایشگاه‌های نوآوری روزنامه‌نگاری برای کمک به شناسایی رسانه‌های مصنوعی و گسترش دسترسی به ابزارهای بررسی علمی رسانه‌ها در حال توسعه هستند. در بیشتر موارد، این ابزارها را باید به‌عنوان نشانه‌هایی حاکی از نیاز به تکمیل روش‌های راستی‌آزمایی خود و مجهز کردن خود به بهترین و به‌روزترین روش‌ها در نظر بگیرید.

ابزارهایی مانند InVID و Forensically می‌توانند به تأیید تصویر به شیوه‌های جستجوی منشأ و تجزیه و تحلیل محدود علمی کمک کنند.

ابزارهای رایگان در این زمینه‌ی کاری عبارتند از:

- **FotoForensics: ابزاری برای بررسی دقیق و علمی عکس‌ها که دارای ظرفیت تجزیه و تحلیل سطح خطا نیز هست و کمک می‌کند بفهمید چه عناصری ممکن است به یک تصویر اضافه شده باشد.**
- **Forensically: مجموعه‌ای از ابزارها برای تشخیص شبیه‌سازی، تجزیه و تحلیل سطح خطا، استخراج فراداده‌های تصویر و کارکردهای دیگر.**

- **InVid: یک افزونه‌ی مرورگر وب که به شما امکان می‌دهد ویدئوها را به فریم تقسیم کنید، جستجوی معکوس تصاویر را در چندین موتور جستجو انجام دهید، فریم‌ها و تصاویر را از طریق یک عدسی بزرگ‌نمایی و کاوش کنید، و فیلترهایی برای بررسی دقیق را روی تصاویر ثابت اعمال کنید.**
- **Reveal Image Verification Assistant:** ابزاری با طیف وسیعی از الگوریتم‌های تشخیص دستکاری تصویر، امکان تجزیه و تحلیل فراداده‌های تصویر، موقعیت جغرافیایی GPS، استخراج تصاویر ریز با فرمت EXIF و ادغام با جستجوی معکوس عکس از طریق گوگل.
- **Ghiro: یک ابزار بررسی دیجیتال آنلاین منبع‌باز.**

توجه داشته باشید که تقریبا همه‌ی این ابزارها برای راستی‌آزمایی تصاویر طراحی شده‌اند، نه ویدئو. این یک ضعف در فضای بررسی و راستی‌آزمایی تصاویر است و بنابراین، برای راستی‌آزمایی ویدئوها هنوز هم لازم است تصاویر تکی‌ای برای تجزیه و تحلیل استخراج شوند. InVID می‌تواند برای این کار به شما کمک کند. این ابزارها بر روی ویدئوهایی با وضوح بالاتر و ویدیوهای غیرفشرده‌ای که مثلا چیزی به آن اضافه یا از آن‌ها حذف شده است، مؤثرتر خواهند بود. هرچه یک ویدئو فشرده‌تر شده باشد یا تعداد دفعات بیشتری ذخیره، یا در رسانه‌های اجتماعی مختلف و پلتفرم‌های به‌اشتراک‌گذاری ویدئو منتشر شده باشد، کارآیی این ابزارها کاهش پیدا می‌کند.

اگر به دنبال ابزارهای بررسی دقیق نوظهوری می‌گردید که برای حل مشکلات ابزارها و شیوه‌های موجود و درنهایت، برای شناسایی دیپ‌فیک‌ها کمکتان کنند، یک گزینه این است که به ابزارهایی که توسط دانشگاهیان و محققان به اشتراک گذاشته می‌شود نگاه کنید. یکی از مراکز تحقیقاتی پیشرو در دانشگاه ناپل، امکان دسترسی آنلاین به کدهای خود برای شناسایی اثر انگشت دوربین (Noiseprint)، تشخیص اتصال تصاویر به هم (Splicebuster) و تشخیص کپی-حرکت و حذف در ویدئوها را به‌صورت رایگان فراهم کرده است.

با پیشرفت رسانه‌های مصنوعی، اشکال جدیدی از بررسی علمی و دقیق تصاویر به‌صورت دستی و خودکار در ابزارهای راستی‌آزمایی موجود که توسط روزنامه‌گاران و راستی‌آزماها استفاده می‌شود و همچنین -به‌طور بالقوه- در روش‌های راستی‌آزمایی از طریق پلتفرم‌ها، ادغام خواهند شد. لازم است

روزنامه‌نگاران دانش خود درباره‌ی جدیدترین ابزارها را به‌روز نگه دارند و درعین‌حال، از وابستگی بیش از حد به این ابزارها پرهیز کنند.

روش‌های بررسی علمی تصاویر مبتنی بر هوش مصنوعی که در حال ظهور هستند

تا اوایل سال ۲۰۲۰ هیچ ابزار تشخیصی مبتنی بر شبکه‌های مولد رقابتی (GAN) که آزمایش خود را پس داده و به‌صورت تجاری موجود باشد، وجود نداشته است. اما بعد از این باید منتظر ورود ابزارهایی به شکل افزایه (Plug-in) و یا به شکل پلتفرم به بازار برای خبرنگاران باشیم. برای بررسی وضعیت فعلی این حوزه و از جمله این ابزارها، می‌توانید کتاب بررسی دقیق رسانه‌ها و دیپ‌فیک‌ها: یک مرور کلی، اثر لوئیزا وردولیوا را بخوانید.

به‌طور کلی این ابزارها متکی به داده‌های آموزشی (نمونه‌هایی) از رسانه‌های مصنوعی مبتنی بر GAN هستند و از آن برای شناسایی نمونه‌های دیگری که با استفاده از تکنیک‌های مشابه تولید می‌شوند استفاده می‌کنند. به‌عنوان مثال، ابزارهایی مانند FaceForensics++ با استفاده از دیپ‌فیک‌های موجود مصرف‌کنندگان، محتوای جعلی تولید می‌کنند و سپس از این حجم زیاد تصاویر جعلی به عنوان داده‌های آموزشی برای الگوریتم‌های تشخیص محتوای جعلی استفاده می‌کنند. این بدان معنا است که این ابزارها ممکن است برای تشخیص آخرین روش‌ها و تکنیک‌های جعل مؤثر نباشند.

این ابزارها برای تشخیص محتوای تولیدشده توسط جی‌ای‌ان بسیار مناسب‌تر از تکنیک‌های فعلی بررسی دقیق خواهند بود. آن‌ها همچنین اشکال جدیدی از ابزارهایی را که با پیشرفت‌های تولید محتوای مصنوعی بهتر سروکار دارند، تکمیل خواهند کرد. بااین‌حال، با توجه به ماهیت رقابتی نحوه‌ی تکامل رسانه‌های مصنوعی، این ابزارها بی‌ایراد نخواهند بود. نکته‌ی کلیدی این است که هر نشانه‌ای از مصنوعی و ساختگی بودن تصاویر باید دوباره بررسی شده و با سایر رویکردهای راستی‌آزمایی نیز تأیید شود.

دیپ‌فیک‌ها و رسانه‌های مصنوعی به سرعت در حال پیشرفت هستند و فناوری‌های مربوطه‌شان تجاری‌سازی شده و دسترسی به آن‌ها و نحوه‌ی استفاده‌شان آسان‌تر می‌شود. محتوای منبع مورد نیاز آن‌ها برای ایجاد تصاویر جعلی از آنچه انتظارش را دارید بسیار کمتر است. در حالی که فناوری‌های

جدید برای تشخیص ظهور می‌کنند و از طریق پلتفرم‌ها و ابزارهای مختلف در اختیار روزنامه‌نگاران/ اطلاعات منبع‌باز قرار می‌گیرند، بهترین راه برای راستی‌آزمایی، استفاده از رویکردهای موجود برای راستی‌آزمایی تصویر/ویدئو، و تکمیل آن‌ها با ابزارهای بررسی دقیقی است که می‌توانند دستکاری تصویر را تشخیص دهند. اعتماد به چشم انسان استراتژی قوی‌ای نیست!

۷. رصد و گزارش‌دهی از محتوای گروه‌های بسته و اپلیکیشن‌های پیام‌رسانی

نوشته‌ی: کلر واردل

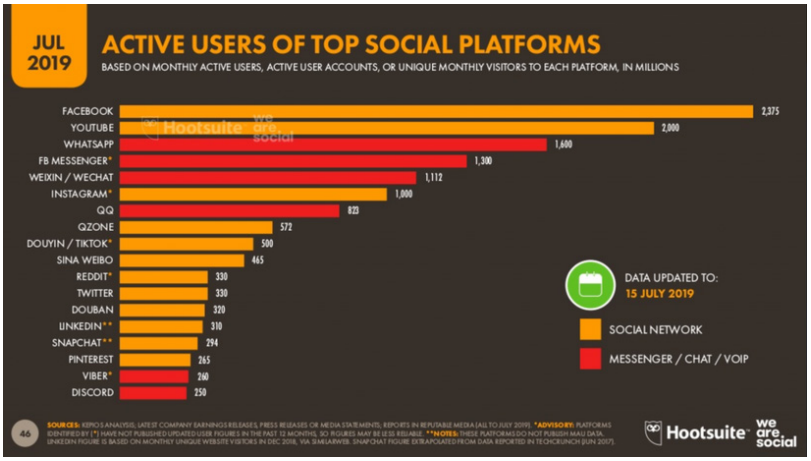
کلر واردل مسئول هدایت استراتژیک و تحقیقات در مؤسسه‌ی فِرْست درفت است، یک سازمان غیرانتفاعی بین‌المللی که کارش پشتیبانی از روزنامه‌نگاران، دانشگاهیان و فناورانی است که برای مقابله با چالش‌های مربوط به اعتماد و حقیقت در عصر دیجیتال تلاش می‌کنند. او عضو مرکز شورنستاین برای رسانه، سیاست و سیاست‌گذاری عمومی در دانشکده‌ی کندی هاروارد، مدیر تحقیقات در مرکز تُوْ برای تحصیلات تکمیلی روزنامه‌نگاری در دانشگاه کلمبیا و رئیس بخش رسانه‌های اجتماعی در کمیساریای عالی سازمان ملل متحد برای پناهندگان است.

در سال ۲۰۱۹، مارک زاکربرگ در مورد «چرخش سیاست‌های فیس‌بوک به سمت حفظ حریم خصوصی کاربران» صحبت کرد، که به این معنی بود که این شرکت آماده است تا تمرکز خود را بر روی گروه‌های فیس‌بوک قرار دهد، زیرا تشخیص می‌داد که مردم به‌شکل فزاینده‌ای به برقراری ارتباط با تعداد کمتری از افراد در فضاهای خصوصی تمایل دارند. در چند سال گذشته، اهمیت گروه‌های کوچک‌تر ارتباطات اجتماعی برای مایی که در این فضا کار می‌کنیم، آشکار شده است.

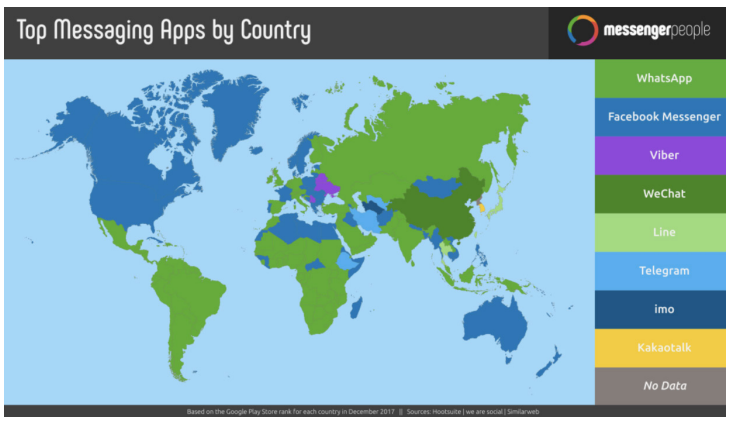
در این فصل توضیحی در مورد پلتفرم‌ها و اپلیکیشن‌های مختلف ارائه خواهم کرد، در مورد چالش‌های نظارت بر این فضاها صحبت می‌کنم و در نهایت، مطلب را با بحث در مورد اخلاق انجام این قبیل تحقیقات به پایان خواهم برد.

پلتفرم‌ها و اپلیکیشن‌های مختلف

تحقیقات اخیر وی‌آر سوشال نشان می‌دهد که فیس‌بوک و یوتیوب هنوز در صدر لیست محبوب‌ترین شبکه‌های اجتماعی هستند، اما سه پلتفرم محبوب بعدی عبارتند از واتس‌اپ، فیس‌بوک مسنجر و وی‌چت.



در بسیاری از مناطق سراسر جهان، اپلیکیشن‌های پیام‌رسانی در حال حاضر منبع اصلی اخبار برای بسیاری از مصرف‌کنندگان هستند، به‌عنوان مثال، اپلیکیشن واتس‌اپ در برزیل، هند و اسپانیا. باوجود اینکه واتس‌اپ و فیس‌بوک مسنجر در سطح جهانی محبوب هستند، در بعضی کشورها استفاده از پیام‌رسان‌های دیگری رایج‌تر است؛ به‌عنوان مثال، در ایران بیشتر از تلگرام، در ژاپن از لاین، در کره‌ی جنوبی از کاکائو تاک و در چین بیشتر از وی‌چت استفاده می‌کنند.



هرکدام از این سایت‌ها از لحاظ رمزگذاری، ویژگی گروه‌ها و داده‌پراکنی و گزینه‌های اضافی مانند فرصت‌های تجارت درون برنامه‌ای، تا حدی عملکردهای متفاوتی دارند.

گروه‌های بسته‌ی فیس‌بوک

سه نوع گروه در فیس‌بوک وجود دارد:

گروه‌های باز یا همگانی، گروه‌های بسته و گروه‌های مخفی

- گروه‌های باز را می‌توان از طریق جستجو پیدا کرد و هر کسی می‌تواند در آن‌ها عضو شود
- گروه‌های بسته نیز در جستجوها پیدا می‌شوند، اما برای عضو شدن باید اول درخواست بدهید
- گروه‌های مخفی را نمی‌توان از طریق جستجو پیدا کرد و عضویت در آن‌ها فقط با دعوت از کاربر امکان‌پذیر است

در مقایسه با گذشته، این روزها افراد بیشتر در گروه‌های فیس‌بوک جمع می‌شوند. بخشی از آن قطعا به دلیل فشاری است که الگوریتم‌های فیس‌بوک بر کاربران وارد می‌کنند؛ اما از طرف دیگر بیشتر افراد خودشان تصمیم می‌گیرند زمان خود را با افرادی بگذرانند که از قبل می‌شناسند و یا افرادی که دیدگاه یا علاقه‌ی مشترکی با آن‌ها دارند.

دیسکورد

بر طبق آمار استاتیستیکا، در جولای ۲۰۱۹، دیسکورد ۲۵۰ میلیون کاربر فعال ماهانه داشت (برای مقایسه، در همان زمان اسنپ ۲۹۴ میلیون، وایبر ۲۶۰ میلیون و تلگرام ۲۰۰ میلیون کاربر داشتند). دیسکورد در میان جامعه‌ی علاقه‌مندان به بازی‌های کامپیوتری محبوب است، اما در سال‌های اخیر به‌عنوان سایتی شناخته شده است که افراد در «سرورهای» آن (شکلی از گروه‌ها در دیسکورد) جمع می‌شوند تا کمپین‌های اطلاعات نادرست را هماهنگ کنند.

یکی از ویژگی‌های دیسکورد و برخی گروه‌های بسته‌ی فیس‌بوک این است که قبل از پذیرش در آن گروه‌ها از شما سوالاتی پرسیده می‌شود. این سوالات ممکن است در مورد حرفه، مذهب، عقاید سیاسی یا نگرش شما نسبت به برخی مسائل اجتماعی باشد.

رمزگذاری، گروه‌ها و کانال‌ها

یکی از دلایل محبوبیت این پلتفرم‌ها و برنامه‌ها ارائه‌ی سطوح مختلف رمزگذاری است. در حال حاضر واتس‌اپ و وایبر، با روش رمزگذاری سرتاسر، امن‌ترین اپلیکیشن‌ها محسوب می‌شوند. در سایر اپلیکیشن‌ها مانند تلگرام، فیس‌بوک مسنجر و لاین استفاده از گزینه‌ی رمزگذاری سرتاسری مستلزم فعال کردن آن است.

برخی از اپلیکیشن‌ها دارای گروه‌ها یا کانال‌هایی هستند که در آن اطلاعات با تعداد زیادی از افراد به اشتراک گذاشته می‌شود. بزرگ‌ترین گروه واتس‌اپ می‌تواند ۲۵۶ نفر را در خود جای دهد. گروه‌های فیس‌بوک مسنجر می‌توانند تا ۲۵۰ عضو داشته باشند. در تلگرام، یک گروه می‌تواند خصوصی یا قابل جستجوی عمومی باشد و تا ۲۰۰ عضو را در خود جای دهد. زمانی که تعداد کاربران به این عدد برسد، امکان تبدیل آن به یک سوپرگروه و افزودن تا ۷۵ هزار کاربر وجود دارد. تلگرام همچنین دارای قابلیت داده‌پراکنی در داخل اپلیکیشن در قالب کانال‌ها نیز هست. شما می‌توانید عضو کانال‌ها شده و محتوایی را که در آن به اشتراک گذاشته می‌شود ببینید، اما نمی‌توانید پاسخی از جانب خود در کانال پست کنید.

نظارت مداوم

شکی نیست که اطلاعات نادرست در برنامه‌های پیام‌رسان بسته نیز منتشر می‌شود. ارزیابی مستقل اینکه آیا اطلاعات نادرست در این پلتفرم‌ها بیشتر از سایت‌های رسانه‌های اجتماعی وجود دارد یا خیر دشوار است، زیرا هیچ راهی برای دیدن آنچه به اشتراک گذاشته می‌شود وجود ندارد. اما همانطور که موارد برجسته از هند، فرانسه و اندونزی به ما نشان داده‌اند می‌دانیم این یکی از ایرادات و مشکلات این پیام‌رسان‌ها است. در ایالات متحده، در جریان تیراندازی در ال‌پاسو و دیتون در آگوست ۲۰۱۹ نیز نمونه‌هایی از شایعات و دروغ‌پردازی‌ها در تلگرام و فیس‌بوک مسنجر را شاهد بودیم.

سؤال این است که آیا لازم است روزنامه‌نگاران، محققان، راستی‌آزماها، کارکنان بهداشتی و انسان‌دوستان در این گروه‌های بسته حضور داشته باشند و انتشار اطلاعات نادرست را زیر نظر بگیرند؟ اگر پاسخ مثبت است، این کار چطور باید به‌گونه‌ای انجام شود که هم اخلاقی باشد و هم امنیت افراد را به خطر نیندازد؟

اگرچه انجام چنین کاری چالش‌های قابل‌توجهی دارد، اما امکان‌پذیر است. این را نیز باید به خاطر داشته باشید که دلیل استفاده‌ی بسیاری از افراد از این پیام‌رسان‌ها برای برقراری ارتباط این است که نمی‌خواهند کاری که می‌کنند رصد شود. آن‌ها از این پیام‌رسان‌ها استفاده می‌کنند چون محتوا در آن رمزگذاری می‌شود و می‌توانند از سطح خاصی از حریم خصوصی برخوردار باشند. این نکته‌ی اساسی برای همه‌ی کسانی است که در این فضاها کار می‌کنند. حتی اگر بتوانید به این فضاها بپیوندید و فعالیت‌هایشان را رصد کنید، مهم است که از مسئولیتی که در قبال شرکت‌کنندگان در این گروه‌ها دارید (که اغلب نمی‌دانند چه کارهایی ممکن است و چه کارهایی نه) آگاه باشید.

تکنیک‌های جستجو

جستجوی این گروه‌ها می‌تواند دشوار باشد، زیرا برای هرکدام پروتکل‌های مختلفی وجود دارد. برای گروه‌های فیس‌بوک، می‌توانید موضوعات را در فیس‌بوک جستجو کرده و سپس نتایج را فیلتر کرده و فقط گزینه‌ی گروه‌ها را انتخاب کنید. اگر می‌خواهید از اپراتورهای جستجوی بولین (Boolean search operators) پیشرفته‌تر (AND , OR , NOT) استفاده کنید، جستجوی خود را با استفاده از کلمات کلیدی در گوگل وارد کنید و سپس site:facebook.com/groups را به عبارت جستجویتان اضافه کنید.

در تلگرام، اگر گوشی‌ای با سیستم عامل اندروید دارید می‌توانید در خود اپلیکیشن جستجو کنید، اما اگر از گوشی‌های آیفون استفاده می‌کنید این امکان برای شما وجود ندارد. بعضی برنامه‌های دسک‌تاپ مانند https://www.telegram- group.com/ وجود دارد که می‌توانید از آن‌ها استفاده کنید. به‌همین‌ترتیب، برای اپلیکیشن دیسکورد هم سایت‌هایی مانند https://disboard.org/search وجود دارد.

تصمیمات در خصوص ملحق شدن و مشارکت

همانطور که قبلا هم اشاره کردیم، بعضی از این گروه‌های بسته برای بالا بردن امنیتْ قبل از ورود سؤالاتی از شما می‌پرسند. قبل از تلاش برای عضویت در گروه‌ها، بهتر است با مدیر یا سردبیر خود درباره‌ی پاسخ‌هایی که باید به سؤالات بدهید مشورت کنید. آیا باید در مورد اینکه که هستید و چرا می‌خواهید عضو گروه شوید حقیقت را بگویید؟ آیا راهی وجود دارد که پاسخ‌های مبهمی بدهید و همچنان بتوانید عضو گروه شوید؟ اگر نه، چگونه می‌توانید تصمیم به پنهان کردن هویت خود را توجیه کنید (اگر می‌خواهید به گروهی بپیوندید که معرفی کردن خود به‌عنوان یک روزنامه‌نگار ممکن است امنیت شما را به خطر بیندازد)؟ اگر به گروه دسترسی پیدا کنید، آیا به طریقی مشارکت نیز خواهید کرد، یا فقط «در کمین» اطلاعاتی خواهید ماند که می‌توانید در جای دیگری راستی‌آزمایی‌اش کنید؟

تصمیم‌گیری درباره‌ی جمع‌آوری خودکار محتوا از گروه‌ها

از طریق جستجوی لینک‌های ارسال‌شده در وب‌سایت‌ها می‌توان گروه‌های باز را پیدا کرد. این گروه‌ها در موتورهای جستجو ظاهر می‌شوند. سپس می‌توان از روش‌های کامپیوتری برای جمع‌آوری خودکار محتوا از این گروه‌ها استفاده کرد. محققانی که بر انتخابات در برزیل و هند نظارت می‌کنند این کار را انجام داده‌اند، و شنیده‌های من حاکی از آن است که سازمان‌های دیگری که کارهای مشابهی انجام می‌دهند نیز از این روش جمع‌آوری خودکار محتوا استفاده می‌کنند.

این تکنیک به سازمان‌ها اجازه می‌دهد چندین گروه را به‌طور هم‌زمان رصد کنند؛ کاری که در غیر این صورت اغلب غیرممکن است. یک نکته‌ی کلیدی این است که تنها درصد کمی از گروه‌ها از این طریق قابل دسترسی هستند و اکثر آن‌ها گروه‌هایی هستند که ناامیدانه به دنبال جذب اعضای بیشتر هستند و بنابراین نماینده‌ی همه‌ی گروه‌ها نیستند. همچنین، این کار برای شخص من نگرانی‌های اخلاقی خاصی را ایجاد می‌کند. با این حال، می‌توان با ایمن کردن داده‌ها، به اشتراک نگذاشتن آن با دیگران و غیر قابل شناسایی کردن پیام‌ها این مشکل را تا حدودی حل کرد. ما برای انجام این نوع کارها به پروتکل‌های مشترک بین‌رشته‌ای نیاز داریم.

ایجاد خطوط تماس برای اطلاع‌رسانی (تیپ‌لاین)

روش دیگر این است که یک خط ارتباطی ایجاد کنید و مردم را تشویق کنید تا محتوا را برای شما ارسال کنند. نکته‌ی کلیدی در خصوص این خطوط ارتباطی، ایجاد یک فراخوان ساده و واضح و توضیح دقیق نحوه‌ی استفاده از محتوایی است که برایتان ارسال می‌شود. آیا از محتوا صرفا برای رصد ترِندها استفاده خواهد شد و یا پس از بررسی مواردی که برایتان ارسال می‌شود، نتیجه‌ی بررسی‌ها را که می‌تواند شامل بی‌اعتبار کردن اطلاعات نادرست باشد، در اختیار عموم قرار خواهید داد؟

اجازه بدهید یک بار دیگر برگردیم به سراغ سؤال‌های اخلاقی‌ای که در کار با گروه‌های بسته تأثیر زیادی دارند. مهم است که در کار با این گروه‌ها فقط در حال دریافت، یا به اصطلاح ,استخراج, محتوا نباشید. حتی اگر اصول اخلاقی را کنار بگذاریم، باز هم تحقیقات نشان می‌دهد اگر مخاطبان ندانند محتوای ارسالی‌شان چگونه مورد استفاده قرار می‌گیرد، احتمال ارسال محتوا از طرف آن‌ها به‌طرز چشمگیری کاهش پیدا می‌کند. افراد زمانی که با آن‌ها مانند شریک رفتار می‌شود تمایل بیشتری به کمک کردن دارند.

اما جنبه‌ی دیگر استفاده از این روش برای جمع‌آوری محتوا این است که امکان ارسال مطالب جعلی در آن بالا است. گاهی نیز ممکن است گروه کوچکی از افراد محتوای مشابهی را در حجم‌های زیاد برای شما ارسال کنند تا مشکلی را بزرگ‌تر از آنچه در واقعیت هست نشان دهند.

اخلاق گزارش‌دهی از گروه‌های بسته در پیام‌رسان‌ها

هنگامی که محتوای مورد نظر خود را پیدا کردید، سؤال این است که چگونه باید در مورد آن گزارش دهید. آیا باید در مورد نحوه‌ی به دست آوردن آن محتوا شفاف باشید؟ در دستورالعمل‌های بسیاری از گروه‌ها تصریح می‌شود محتوایی که در گروه به اشتراک گذاشته شده و در مورد آن بحث می‌شود، نباید به خارج از گروه انتقال پیدا کرده و در مقیاس کلان‌تر به اشتراک گذاشته شود. اگر گروه مورد نظر پر باشد از اطلاعات نادرست، گزارش‌دهی شما درباره‌ی آن چه عواقبی خواهد داشت؟ آیا می‌توانید آنچه را که در گروه‌ها یا فضاهای آنلاین پیدا کرده‌اید تأیید کنید؟ اگر در خصوص این محتوا گزارشی تهیه کنید، آیا ممکن است امنیت خود، همکاران یا خانواده‌تان را به خطر بیندازید؟ به یاد داشته

باشید که افشاء کردن هویت روزنامه‌نگاران و محققان (یا بدتر از آن) یکی از روش‌های معمول برخی از گروه‌های بدکار آنلاین است.

نتیجه‌گیری

گزارش‌دهی از محتوای اپلیکیشن‌ها و گروه‌های بسته در پیام‌رسان‌ها و درباره‌ی آن‌ها پر از چالش است، اما این منابع به‌عنوان مکان‌هایی که اطلاعات در آن به اشتراک گذاشته می‌شود، اهمیت فزاینده‌ای پیدا می‌کنند. به‌عنوان اولین قدم، به سوالات مطرح شده در این فصل فکر کنید، با همکاران و سردبیر خود صحبت کنید، و اگر اتاق خبر شما دستورالعمل‌هایی در مورد این نوع گزارش‌ها ندارد، دست‌به‌کار شوید و روی بعضی دستورالعمل‌های کلی کار کنید. هیچ قانون استانداردی در مورد نحوه‌ی انجام این کار وجود ندارد. بسته به داستان گزارش، بستر آن، شخص گزارشگر و دستورالعمل‌های تحریریه‌ی اتاق خبر قوانین می‌تواند متفاوت باشد. اما مهم است که قبل از شروع این نوع گزارش، تمام جزئیات در نظر گرفته شود.

۷.الف. مطالعه‌ی موردی: بولسونارو در بیمارستان

نوشته‌ی: سرژو لوتسکی

سرژو لوتسکی روزنامه‌نگار و سردبیر پروژه‌ی کومپرُوا است، ائتلافی از ۲۴ سازمان رسانه‌ای که به‌طور مشترک برای بررسی شایعات در مورد سیاست عمومی در برزیل کار می‌کنند. در سال ۲۰۱۸، کومپرُوا یک محتوای مشکوک به اشتراک گذاشته شده در رسانه‌های اجتماعی و اپلیکیشن‌های پیام‌رسانی در مورد انتخابات ریاست جمهوری برزیل را بررسی کرد.

روز ۶ سپتامبر ۲۰۱۸، یک ماه قبل از انتخابات ریاست جمهوری برزیل، ژائیر بولسونارو، نامزد راست افراطی، یک رویداد تبلیغاتی در مرکز شهر جویز دو فورا، شهری با ۵۶۰ هزار نفر جمعیت در ۲۰۰ کیلومتری ریودوژانیرو، برگزار کرد.

یک هفته از پیشی گرفتن بولسونارو بر رقیبش در دور اول رأی‌گیری‌های انتخابات ریاست جمهوری برزیل گذشته بود. بعد از اینکه رئیس جمهور سابق، لوئیز ایناسیو لولا داسیلوا، توسط دادگاه عالی الکترال از نامزدی مجدد برای انتخابات ریاست‌جمهوری منع شد، بولسونارو جایگاه اول را به دست آورد.

بااین‌حال، تخمین‌ها نشان می‌داد که بولسونارو در دور دوم از چهار کاندیدایی که در نظرسنجی‌ها میزان آرایی نزدیک به آرای او داشتند شکست خواهد خورد.

وضعیت بولسونارو نگران‌کننده بود، زیرا او روزانه تنها دو بلوک ۹ ثانیه‌ای در تبلیغات رایگان انتخاباتی در تلویزیون داشت. قوانین انتخاباتی برزیل، ایستگاه‌های رادیویی و تلویزیونی را ملزم می‌کنند که بخشی از زمان خود را به‌صورت رایگان برای تشریح وعده‌های انتخاباتی به مردم در اختیار احزاب سیاسی قرار دهند. این زمان بر اساس تعداد کرسی‌های کسب‌شده توسط هر حزب در آخرین انتخابات مجلس نمایندگان توزیع می‌شود. تعداد کم کرسی‌های حزب بولسونارو به این معنا بود که زمان پخش رایگان بسیار کمی نصیب او خواهد شد. در نتیجه، او مجبور بود به حامیان خود در شبکه‌های اجتماعی تکیه کند و با رأی‌دهندگان در خیابان‌ها ارتباط مستقیم برقرار کند.

بولسونارو در شهر جویز دو فورا، مانند شهرهای دیگری که قبلا از آن‌ها بازدید کرده بود، در یک راهپیمایی شرکت کرد و هوادارانش او را بر دوش گرفتند. جمعیتی از هواداران هم آن‌ها را دنبال می‌کردند که راهپیمایی ناگهان متوقف شد. مردی از میان جمعیت بیرون آمد و به نامزد ریاست جمهوری چاقو زد. چاقو زخم عمیقی در ناحیه‌ی شکم بولسونارو بر جای گذاشت و سیلی از اتفاقات را در شبکه‌های اجتماعی رقم زد.

بازار شایعات و تئوری‌های توطئه حسابی گرم شده بود و برخی آدلیو بیسپو دی اولیویرا، مردی که بولسونارو را با چاقو زخمی کرده بود، را به ارتباط داشتن با حزب رئیس‌جمهور سابق، دیلما روسف که در سال ۲۰۱۶ از ریاست جمهوری برکنار شد، متهم کردند. عکس‌هایی جعلی منتشر شدند که مهاجم را در کنار لولا نشان می‌دادند. بیسپو با حزب چپ‌گرای سوسیالیسم و آزادی (PSOL) مرتبط فرض می‌شد و امتناع وکلای او از گفتن اینکه چه کسی هزینه‌های آن‌ها را پرداخت می‌کند، فقط به ادعاهای توطئه‌آمیز بیشتر دامن می‌زد.

در همان زمان، ویدئوها و پیام‌هایی که سعی در تضعیف موقعیت بولسونارو داشتند نیز در رسانه‌های اجتماعی مورد توجه قرار گرفتند. برخی از این محتواهای مخرب ادعا می‌کردند که چاقو خوردن بولسونارو صحنه‌سازی بوده است و او درواقع برای درمان سرطان در بیمارستان بستری بوده است و عکس‌های منتشر شده از جراحی او نیز جعلی بوده است.

چاقو خوردن بهانه‌ی موجهی به دست بولسونارو داد تا از شرکت در فعالیت‌های تبلیغاتی شانه خالی کند، اما درعین‌حال موقعیت او را در رأی‌گیری‌ها بهبود بخشید (و البته، سرانجام نیز در انتخابات پیروز شد).

در ۱۹ سپتامبر و تقریبا دو هفته پس از حمله به بولسونارو، گروهی به نام الهسوییس سم فِیک (Eleições sem Fake) که توسط دانشگاه فدرال میناس گرایس برای رصد گروه‌های واتس‌اپی راه‌اندازی شده بود متوجه فایل صوتی‌ای شد که در گروه‌ها دست‌به‌دست می‌شد. این فایل صوتی توسط ۱۶ گروه از ۳۰۰ گروهی که این پروژه آن‌ها را رصد می‌کرد به اشتراک گذاشته شده بود؛ برخی از این گروه‌ها حامی بولسونارو بودند.

همان روز سازمان ما، کومپرُوا، درخواست‌هایی از خوانندگان دریافت کرد که خواهان تأیید اصالت

محتوای فایل صوتی بودند.

در این فایل صوتی که کمی طولانی‌تر از یک دقیقه بود، مردی عصبانی با صدایی شبیه صدای بولسونارو با فردی که به نظر می‌رسید پسرش ادواردو باشد، بحث می‌کرد و از اینکه در بیمارستان نگه داشته شده شکایت می‌کرد. در فایل صوتی، مرد می‌گفت که دیگر نمی‌تواند «این نمایش مسخره» را تحمل کند، و به طور ضمنی می‌گفت که کل ماجرا صحنه‌سازی بوده است.

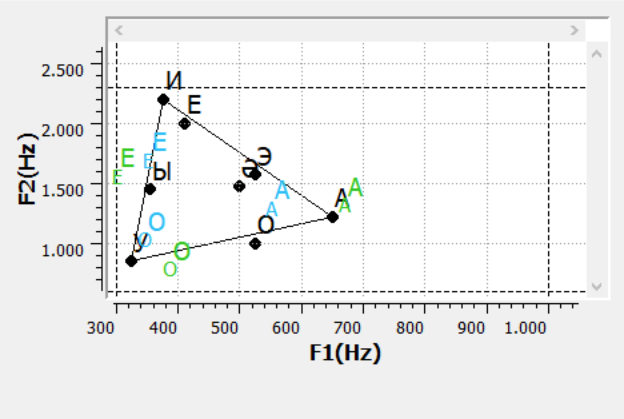
آن روز، بولسونارو هنوز در بخش مراقبت‌های نیمه‌ویژه‌ی بیمارستان آلبرت انیشتین در سائوپائولو بستری بود. گزارش پزشکی گفته بود که او تب ندارد، تغذیه داخل وریدی دریافت می‌کند و عملکرد روده‌اش بهبود یافته است.

کومپرُوا موفق نشد منبع اصلی انتشار فایل صوتی را پیدا کند. این فایل صوتی ابتدا در واتس‌اپ و در زمانی منتشر شده بود که هنوز امکان به اشتراک گذاشتن فایل‌ها در حداکثر ۲۰ مکالمه وجود داشت. این باعث شد فایل به سرعت پخش شود و به شبکه‌های اجتماعی دیگر نیز راه پیدا کند. و به‌این‌ترتیب، تشخیص منبع اصلی به‌اشتراک‌گذاری آن غیرممکن شد. (از آن زمان، واتس‌اپ تعداد افرادی که می‌توانید پیامی را به آن‌ها فوروارد کنید محدود کرده است).

بعد از آنکه کومپرُوا موفق نشد پخش‌کننده‌ی فایل صوتی را شناسایی کند، تصمیم بر آن شد که بر شیوه‌های سنتی‌تر تحقیقات متمرکز شویم و به همین دلیل، از مؤسسه‌ی تحقیقات قانونی برزیل (Instituto Brasileiro de Perícia) برای تهیه‌ی یک گزارش تخصصی درخواست کمک کردیم.
کارشناسان صدای موجود در فایل صوتی را با مصاحبه‌ای که در آوریل ۲۰۱۸ از بولسونارو ضبط شده بود مقایسه کردند و به این نتیجه رسیدند که صدای حاضر در فایلی که در شبکه‌های اجتماعی پخش شده بود، از آن بولسونارو نیست.

کارشناسان یک تجزیه و تحلیل کیفی از صدا، گفتار و نشانگرهای زبانی مردی که در فایل صوتی صحبت می‌کرد انجام دادند. سپس این پارامترها را در هر دو نمونه با هم مقایسه کردند. در این تحلیل، آن‌ها الگوهای بیان مصوت‌ها و صامت‌ها، ریتم و سرعت گفتار، الگوهای لحن گفتار، کیفیت صدا، عادات کلامی گوینده و همچنین استفاده از کلمات و قواعد دستوری خاص را مورد بررسی قرار دادند.

به‌عنوان مثال، تصویر زیر تجزیه و تحلیل فرکانس «سازنده‌ها» را نشان می‌دهد، یعنی زیر و بم‌های ایجاد شده توسط ارتعاشات مجرای صوتی (حفره‌ای که در آن صدای تولید شده در حنجره فیلتر می‌شود). هوای داخل مجرای صوتی، بسته به اندازه و شکل دهانه‌ی آن، در گام‌های متفاوتی به ارتعاش درمی‌آید. تصویر زیر تجزیه و تحلیل فرکانس سازندها را با استفاده از مصوت‌های اِ، اَ و اُ نشان می‌دهد. مصوت‌های سبزرنگ مطابق با فایل صوتی‌ای است که در واتس‌اپ به دست آوردیم و مصوت‌های آبی‌رنگ مربوط به نمونه‌ای است که از مصاحبه‌ی بولسونارو مربوط به چند روز قبل از حمله گرفته شده است.



تجزیه و تحلیل‌های بیشتر نشان داد که سخنگوی فایل صوتی واتس‌اپ دارای لهجه‌ی منطقه‌ی خاصی از حومه‌ی ایالت سائوپائولو است؛ لهجه‌ای که در تجزیه و تحلیل صدای بولسانورو دیده نمی‌شد. در نمونه‌های بررسی شده تفاوت‌هایی در رزونانس، چگونگی تولید آواها، سرعت گفتار و انحراف آوایی تشخیص داده شد.

کومپرُوا با کارشناس دیگری نیز مشورت کرد. این کارشناس نیز به این نتیجه رسید که صدای ضبط شده به دلایل مختلفی با صدای بولسونارو متفاوت است. به عقیده‌ی او، تن صدای سخنگوی فایل صوتی در مقایسه با تن صدای بولسونارو زیرتر است. به‌علاوه، سرعت کلام نیز در مقایسه با ویدئوی دیگری که از این نامزد در بیمارستان ضبط شده بود، سریع‌تر بود.

یکی دیگر از شواهدی که نشان می‌داد فایل صوتی مذکور جعلی است، پایین بودن کیفیت آن است.

به گفته‌ی کارشناسان باتجربه، این یک ترفند ساده و معمول است: کاهش وضوح صداها، فیلم‌ها و عکس‌ها تجزیه و تحلیل آن‌ها را دشوارتر می‌کند.

و اما پاسخ بولسونارو به انتشار این فایل صوتی؛ پسران بولسونارو، فلاویو و کارلوس، پاسخ خود را در رسانه‌های اجتماعی پست کردند و گفتند که این فایل صوتی یک «خبر جعلی» است.

اگر این فایل صوتی امروز در فضای مجازی پخش می‌شد، احتمالا باور این که صدا متعلق به بولسونارو است سخت‌تر بود. قبل از انتخابات، با تنها ۱۸ ثانیه فرصت در روز برای حضور در تلویزیون و غیبت در مناظره‌های تبلیغاتی به دلیل بستری شدن در بیمارستان و درمان، صدای رئیس‌جمهور فعلی چندان شناخته‌شده نبود. این فرصتی را برای ایجاد یک فایل صوتی جعلی ایجاد کرد که بسیاری را فریب داد.

بااین‌حال، با گذشت بیش از یک سال، هنوز درک این موضوع دشوار است که چرا گروه‌های طرفدار بولسونارو و مبارزات انتخاباتی‌اش این فایل صوتی را به اشتراک گذاشتند؛ فایلی که اگر صحت آن ثابت می‌شد، می‌توانست نامزدی او را از بین ببرد. ما هرگز به‌طور کامل نخواهیم فهمید که چرا این گروه‌ها این محتوا را تا این حد مشتاقانه به اشتراک می‌گذاشتند. بااین‌حال، این ماجرا حاکی از این واقعیت است که محتوایی که ادعایی تا این حد غافلگیرکننده را مطرح می‌کند به‌سرعت در رسانه‌های اجتماعی پخش خواهد شد.

۸. بررسی وب‌سایت‌ها

نوشته‌ی: **کرگ سیلورمن**

کرگ سیلورمن سردبیر سایت خبری بازفید است و رهبری این وب‌سایت محبوب را که اخبار مربوط به پلتفرم‌های جهانی، اطلاعات نادرست در فضای مجازی و گمراه‌سازی‌های رسانه‌ای را پوشش می‌دهد، بر عهده دارد. او پیش از این کتابچه‌ی راهنمای راستی‌آزمایی و همچنین کتابچه‌ی راهنمای صحت‌سنجی در روزنامه‌نگاری تحقیقی را گردآوری و ویرایش کرده و مؤلف کتاب دروغ‌ها، دروغ‌های لعنتی و محتوای پربازدید: چگونه وب‌سایت‌های خبری شایعات، ادعاهای غیرمستند و اطلاعات نادرست را در فضای مجازی پراکنده (و یا بی‌اعتبار) می‌کنند نیز هست.

وب‌سایت‌ها گاهی توسط افرادی که هدفشان کسب درآمد، جمع‌آوری ایمیل‌ها و سایر اطلاعات شخصی یا ایجاد یک پایگاه آنلاین است مورد استفاده قرار می‌گیرند. روزنامه‌نگاران باید با نحوه‌ی بررسی پایگاه‌های فضای مجازی آشنا باشند و در صورت امکان، آن را به عملیات بزرگ‌تری که ممکن است شامل حساب‌های رسانه‌های اجتماعی، برنامه‌ها، شرکت‌ها یا سایر نهادها باشد متصل کنند.

به یاد داشته باشید که متن، تصاویر یا حتی کل وب‌سایت ممکن است در طول زمان - به خصوص پس از شروع تماس با افراد و پرسیدن سوالاتی از آن‌ها- ناپدید شوند. بهترین روش این است که از Wayback Machine برای ذخیره‌ی صفحات مهم در وب‌سایت هدف خود استفاده کنید. اگر صفحه‌ای به‌درستی در این برنامه ذخیره نمی‌شود، از ابزاری مانند archive.today استفاده کنید. به‌این‌ترتیب می‌توانید به صفحات آرشیو شده به‌عنوان مدرکی بر آنچه پیدا کرده‌اید لینک بدهید و از دادن لینک مستقیم به سایتی که اطلاعات نادرست/دروغ را منتشر می‌کند، اجتناب کنید (Hunch-ly یک ابزار پولی عالی برای ایجاد آرشیو شخصی صفحات وب به صورت خودکار در حین کار است). این ابزارهای بایگانی همچنین برای بررسی تغییرات یک وب‌سایت در طول زمان نیز ضروری هستند. توصیه‌ی من این است که افزونه‌ی مرورگر Wayback Machine را هم نصب کنید تا آرشیو کردن صفحات و مشاهده‌ی نسخه‌های قبلی برایتان آسان‌تر باشد.

یکی دیگر از افزونه‌های مفید مرورگر Ghostery است که ردیاب‌های (Tracker) موجود در یک صفحه‌ی وب را به شما نشان می‌دهد. این کمکتان می‌کند به سرعت تشخیص دهید که آیا سایتی از گوگل آنالتیکس و/یا شناسه‌های گوگل اَدسِنس استفاده می‌کند یا خیر؛ اطلاعاتی که برای استفاده از تکنیک‌های ذکر شده در زیر به شما کمک خواهد کرد.

در این فصل، به چهار دسته اطلاعات مرتبط برای بررسی وب‌سایت‌ها نگاهی خواهیم انداخت:

محتوا، کد، تجزیه و تحلیل، ثبت نام و عناصر متصل.

محتوا

اکثر وب سایت‌ها دست‌کم اندکی توضیحات در مورد خود در اختیار شما قرار می‌دهند. چه این توضیحات در یک صفحه‌ی اختصاصی با عنوان «درباره‌ی ما» باشد و چه در پایین صفحه‌ی اصلی یا جای دیگری آورده شده باشد، جای خوبی برای شروع است. درعین‌حال، فقدان اطلاعات واضح می‌تواند حاکی از این باشد که سایت با عجله ایجاد شده است یا صاحبان آن سعی دارند جزئیات مربوط به مالکیت و هدف خود را پنهان کنند.

علاوه بر خواندن هر متنی تحت عنوان «درباره‌ی ما»، یک بررسی کامل از محتوای وب‌سایت نیز انجام دهید؛ اینکه چه کسی آن را اداره می‌کند، هدف چیست و آیا وب‌سایت مورد نظر بخشی از یک شبکه یا پروژه‌ی بزرگ‌تر است یا خیر. برخی از مواردی که باید به دنبال آنها باشید عبارتند از:

- **آیا شخص حقیقی یا حقوقی خاصی به‌عنوان مالک وب‌سایت معرفی شده و بخشی تحت عنوان «درباره‌ی ما» دارد یا خیر؟**
- **آیا نام شرکت یا شخص خاصی در هشدار حق نشر در انتهای صفحه‌ی اصلی یا هر صفحه‌ی دیگری ذکر شده است؟**
- **آیا نام اشخاص، نشانی یا نام نهادهای خاصی در قسمت مقررات حفظ حریم خصوصی یا شرایط و ضوابط ذکر شده است؟ آیا این نام‌ها یا شرکت‌ها با آنچه در پایین صفحات یا**

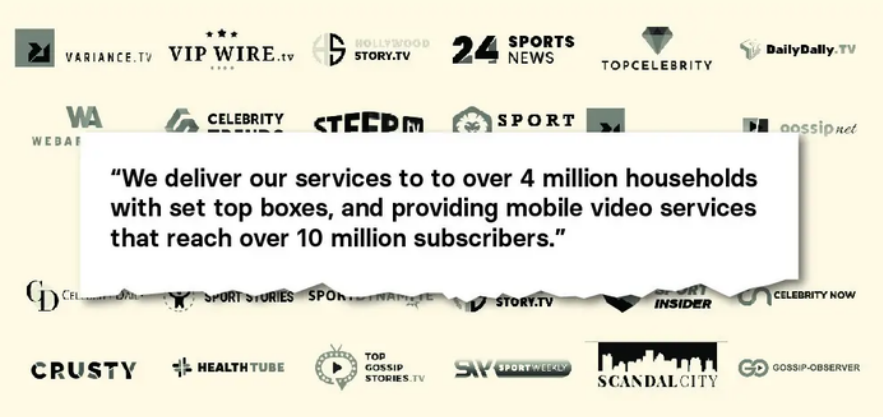
مکان‌های دیگر در سایت ذکر شده است متفاوت هستند؟

- **اگر سایت مقالاتی را منتشر می‌کند، ببینید آیا مقالات دارای امضاء و یا لینک‌های قابل کلیک هستند یا خیر. اگر چنین است، ببینید آیا لینک‌ها به صفحه‌ای با اطلاعات بیشتر، مانند بیوگرافی نویسنده یا لینک‌هایی به حساب‌های اجتماعی نویسنده متصل هستند یا خیر.**
- **آیا حساب‌های کاربری شبکه‌های اجتماعی‌ای که با سایت مرتبط باشند در آن ذکر شده‌اند؟ اشاره به حساب‌های شبکه‌های اجتماعی می‌تواند در قالب آیکون‌های کوچک در بالا، پایین یا حاشیه‌های صفحه و یا به‌صورت تگ embed باشد که از شما دعوت می‌کند صفحه‌ی فیس‌بوک وب‌سایت را لایک کنید. اگر صفحه آیکون‌های پلتفرم‌هایی مانند فیس‌بوک و توییتر را نشان می‌دهد، نشانگر ماوس خود را روی آن‌ها ببرید و به سمت چپْ پایینِ پنجره‌ی مرورگر خود نگاه کنید تا URL مرتبط با آیکون‌ها را ببینید. اغلب زمانی که وب‌سایتی با عجله ایجاد می‌شود، سازنده زحمت پر کردن تمام گزینه‌های شبکه‌های اجتماعی در قالب پیش‌ساخته را به خود نمی‌دهد. در این صورت، در پایین سمت چپ مرورگر فقط لینک facebook.com را بدون نام کاربری خواهید دید.**
- **آیا سایت محصولات، مشتریان، قدردانی‌ها یا نام افراد و شرکت‌های دیگری را که ممکن است با آن ارتباط داشته و ارزش بررسی داشته باشند را ذکر کرده است؟**
- **مطمئن شوید نه فقط صفحه‌ی اصلی، بلکه تمام صفحات وب‌سایت را بررسی کرده‌اید. روی همه‌ی منوهای اصلی کلیک کنید و تا پایین صفحه بروید تا صفحات دیگری که ارزش بازدید دارند را از قلم نیندازید.**

بخش مهمی از بررسی محتوا به بررسی اصالت آن مربوط می‌شود. آیا اطلاعاتی که در بخش «درباره‌ی ما» آمده از جای دیگری کپی شده است؟ آیا وب‌سایت در حال پخش اطلاعات نادرست یا گمراه‌کننده است و یا از موضوع خاصی حمایت و آن را تقویت می‌کند؟

در سال ۲۰۱۸، من تحقیقاتی درباره‌ی یک طرح بزرگ کلاهبرداری تبلیغات دیجیتال، که شامل اپلیکیشن‌های موبایل و وب‌سایت‌های محتوا و همچنین شرکت‌های پوششی و کارمندان و

شرکت‌های جعلی بود، انجام دادم. در نهایت موفق شدم بیش از ۳۵ وب‌سایت را که با این طرح در ارتباط بودند شناسایی کنم. یکی از راه‌های پیدا کردن این وب‌سایت‌های مرتبط، کپی کردن متن موجود در بخش «درباره‌ی ما» و وارد کردن آن در موتور جستجوی گوگل بود. با این کار موفق شدم بلافاصله ۲۰ وب‌سایت را که همگی از متن مشابهی استفاده کرده بودند پیدا کنم:

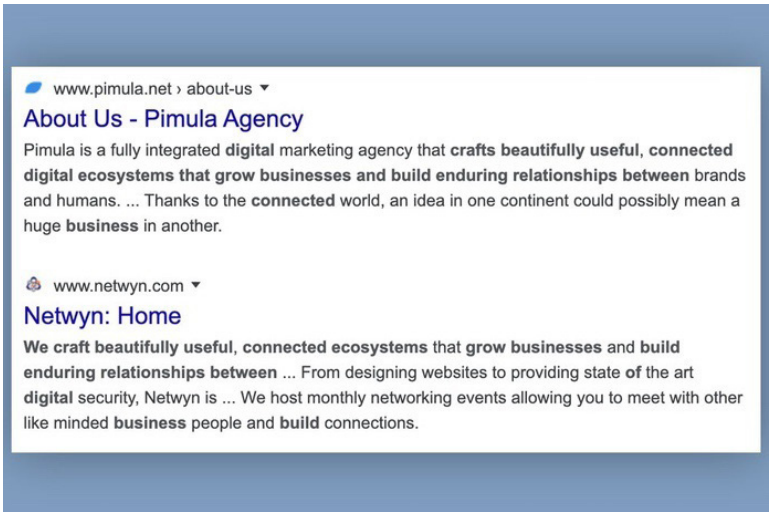


کلاهبرداران مجری این طرح برای شرکت‌های صوری خود وب‌سایت‌هایی هم طراحی کرده بودند تا شرکای بالقوه در شبکه‌های تبلیغاتی بتوانند هنگام انجام بررسی‌های احتیاطی از این وب‌سایت‌ها دیدن کنند. یک نمونه از این شرکت‌های صوری شرکتی به اسم آتوسس بود که در صفحه‌ی اصلی وب‌سایت آن نام چند کارمند با عکس پرسنلی آن‌ها آورده شده بود. جستجوی معکوس عکس‌ها در Yandex (بهترین ابزار جستجوی تصویر برای چهره‌ها) به سرعت نشان داد که بیشتر آن‌ها تصاویر استوک هستند:

آتوسس همچنین این متن را در پسایند (پایین صفحه) سایت خود آورده است:

«ما اکوسیستم‌های بسیار مفید و به هم‌پیوسته‌ای را ایجاد می‌کنیم که باعث رشد کسب و کار و ایجاد روابط پایدار بین رسانه‌های آنلاین و کاربران می‌شود.»

همین عبارت را می‌توان بر روی وب‌سایت‌های دست‌کم دو شرکت بازاریابی دیگر نیز مشاهده کرد:



اگر شرکتی به جای تصاویر کارمندان واقعی از تصاویر استوک و به جای متن‌های اصیل و متعلق به خود شرکت از سرقت ادبی استفاده می‌کند، باید بدانید آن چیزی نیست که ادعا می‌کند.

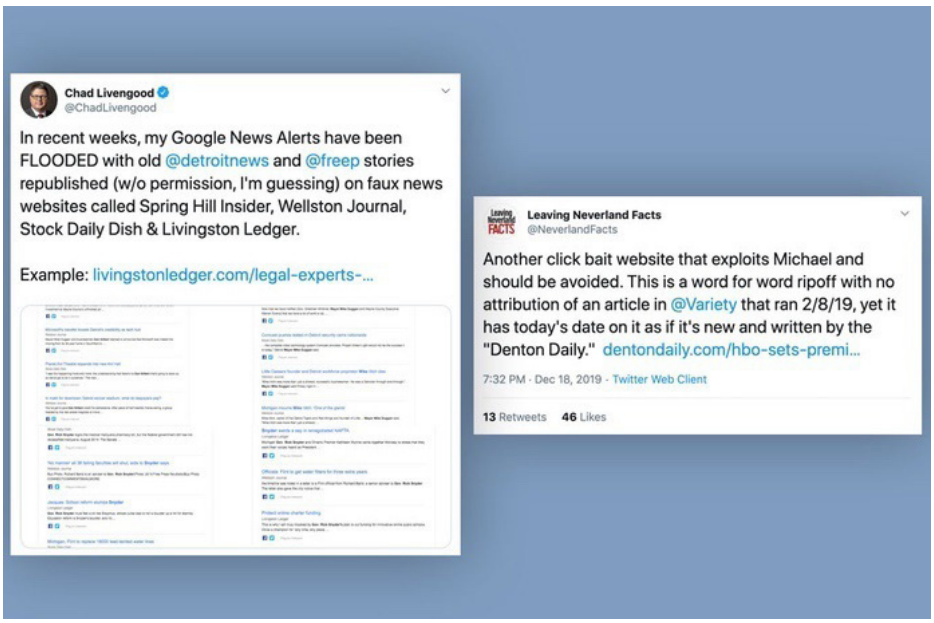
به‌علاوه، بهتر است متنی را از یکی از مقالات سایت کپی و آن را در گوگل یا موتور جستجوی دیگری وارد کنید. گاهی اوقات سایتی که ادعا می‌کند منبع اخبار است درواقع فقط از رسانه‌های واقعی سرقت ادبی می‌کند.

در سال ۲۰۱۹، با سایتی به نام forbesbusinessinsider.com برخورد کردم که در نگاه اول به نظر می‌رسید یک سایت خبری است که اخبار حوزه‌ی فناوری را پوشش می‌دهد. اما درواقع، کار این وب‌سایت سرقت انبوه مقالات از رسانه‌های مختلف بود و از جمله، به طرز خنده‌داری، مقاله‌ای که خودم در مورد وب سایت‌های محلی جعلی نوشته بودم نیز روی این وب‌سایت وجود داشت.

یک گام ابتدایی دیگر در تحقیقات، کپی کردن URL وب‌سایت و جستجوی آن در گوگل است. به‌عنوان مثال، "forbesbusinessinsider.com". از این طریق می‌توانید ببینید چه تعداد از صفحات

وب‌سایت ایندکس شده‌اند، و همچنین ممکن است به نمونه‌هایی از افراد دیگری برخورد کنید که سایت را گزارش کرده یا در مورد آن صحبت کرده‌اند. همچنین می‌توانید با بارگیری صفحه اصلی Google News و وارد کردن "forbesbusinessinsider.com" در کادر جستجو، بررسی کنید که آیا وب‌سایت مورد نظرتان در Google News فهرست شده است یا خیر.

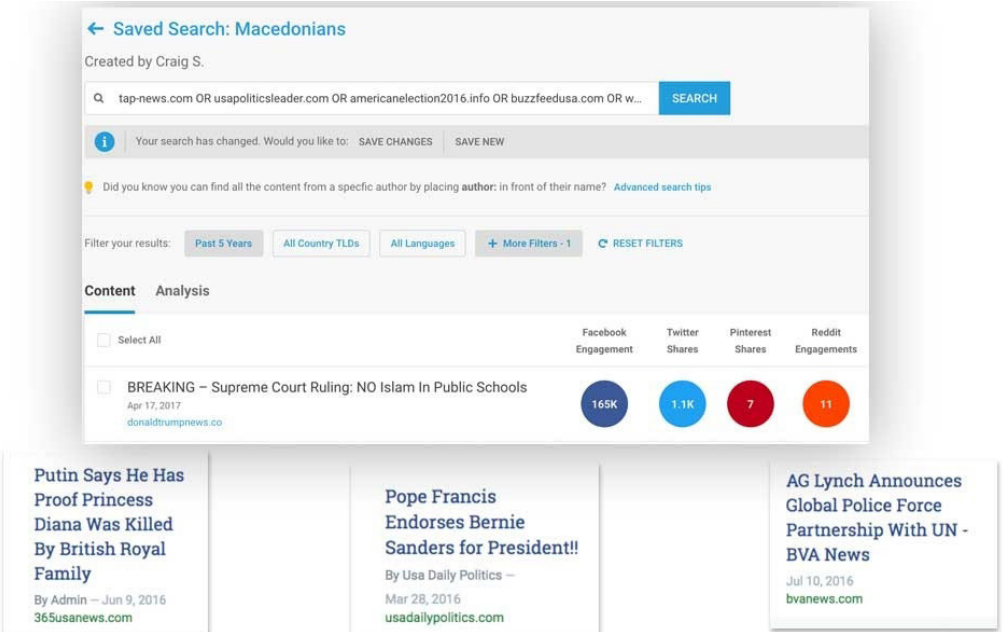
روش دیگر این است که URL سایت را بردارید و آن را در نوارهای جستجو در Twitter.com یا Facebook.com وارد کنید. این به شما نشان خواهد داد که آیا افرادی به سایت لینک داده‌اند یا خیر. طی یک تحقیق، با وب سایت dentondaily.com برخورد کردم. صفحه‌ی اصلی آن تنها چند مقاله را از اوایل سال ۲۰۲۰ نشان می‌داد، اما وقتی URL آن را در توئیتر جستجو کردم، متوجه شدم که وب‌سایت قبلا محتوای سرقت ادبی منتشر کرده بوده و همین باعث شده بود افرادی که متوجه شده بودند محتوای سایت را گزارش و از آن شکایت کنند. این مقالات قدیمی‌تر از سایت حذف شده بودند، اما توئیت‌ها شواهدی از رفتار قبلی وب‌سایت را ارائه می‌کرد.



هنگامی که محتوای یک وب‌سایت را به‌خوبی بررسی کردید، نوبت به آن می‌رسد که نحوه‌ی انتشار آن را درک کنید. **در اینجا با دو ابزار برای این کار آشنا خواهیم شد: BuzzSumo و CrowdTangle.**

در سال ۲۰۱۶، با محققی به نام لارنس الکساندر برای بررسی سایت‌های خبری سیاسی آمریکایی که از خارج از کشور اداره می‌شوند، همکاری کردم. چندی نگذشت که تحقیقاتمان توجه ما را به سمت وب‌سایت‌هایی جلب کرد که از وِلِس در مقدونیه‌ی شمالی اداره می‌شدند. با استفاده از جزئیات ثبت دامنه (جزئیات بیشتر در این‌باره در ادامه) موفق به کشف بیش از صد وب‌سایت مربوط به اخبار سیاسی آمریکا شدیم که از این شهر اداره می‌شدند. من می‌خواستم ایده‌ای از میزان محبوبیت آن‌ها و نوع داستان‌هایی که منتشر می‌کنند به دست بیاورم. آدرس URL چندین سایت را، که به نظر می‌رسید فعال‌ترین‌ها هستند، گرفتم و در BuzzSumo جستجو کردم؛ ابزاری که می‌تواند فهرستی از محتوای یک وب‌سایت را براساس میزان تعامل با آن در فیس‌بوک، توئیتر، پینترست و ردیت نشان دهد. (این ابزار یک نسخه‌ی رایگان دارد، اما محصول پولی نتایج بسیار بیشتری ارائه می‌دهد).

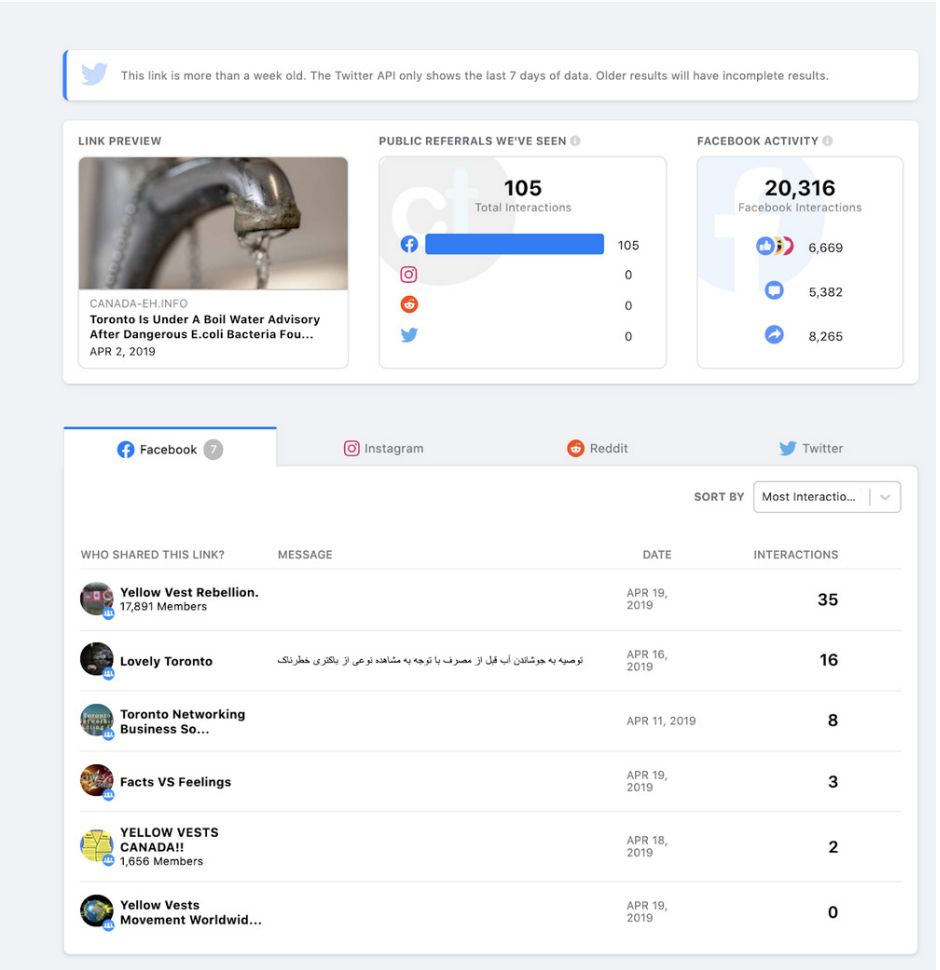
بلافاصله متوجه شدم مقالاتی از این سایت‌ها که بیشترین تعامل را در فیس‌بوک دارند کاملا دروغین هستند. این اطلاعات نقش بسیار کلیدی‌ای داشتند و زاویه‌ی دیدی متفاوت با گزارش‌های قبلی را در اختیار ما قرار دادند. تصویر زیر صفحه‌ی اصلی نتایج جستجوی BuzzSumo را نشان می‌دهد که مشارکت‌های فیس‌بوک، توئیتر، پینترست و ردیت برای یک سایت خاص و همچنین برخی از نمونه‌های داستان‌های نادرست سال ۲۰۱۶ را فهرست می‌کند:



یک راه دیگر برای شناسایی نحوه‌ی انتشار محتوای یک وب‌سایت در فیس‌بوک، توئیتر، اینستاگرام و ردیت، نصب افزونه مرورگر رایگان CrowdTangle یا استفاده از ابزار جستجوی لینک مبتنی بر وب آن است. هر دو امکانات یکسانی را ارائه می‌دهند، اما ما اینجا با نسخه‌ی وب کار خواهیم کرد (این ابزارها رایگان هستند، اما برای استفاده از آن‌ها به یک حساب کاربری فیس‌بوک نیاز دارید).

تفاوت اصلی بین BuzzSumo و CrowdTangle این است که می‌توانید URL یک سایت را در BuzzSumo وارد کنید و این ابزار به‌طور خودکار پرتعامل‌ترین محتوای آن سایت را نمایش خواهد داد. CrowdTangle برای بررسی یک URL خاص در یک وب‌سایت استفاده می‌شود. بنابراین اگر buzzfeednews.com را در CrowdTangle وارد کنید، آمار تعامل را فقط برای همان صفحه‌ی اصلی دریافت خواهید کرد، در حالیکه BuzzSumo کل دامنه را برای پیدا کردن محتوایی که بیشترین تعامل را دریافت کرده اسکن می‌کند. تفاوت دیگر این است که افزونه‌ی مرورگر و ابزار جستجوی مبتنی بر وب CrowdTangle تعاملات توئیتر را فقط از هفت روز گذشته نشان می‌دهند. BuzzSumo تمام دفعاتی را که مقالات وب‌سایت مورد نظر در توئیتر اشتراک‌گذاری شده‌اند نشان می‌دهد.

به‌عنوان مثال، من URL یک داستان قدیمی و نادرست در مورد هشدار مقامات درباره‌ی کیفیت آب آشامیدنی و لزوم جوشاندن آن در تورنتو را در CrowdTangle وارد کردم (وب‌سایت منتشرکننده بعدا داستان را حذف کرد اما URL آن هنوز و تا زمان نوشتن این مقاله فعال است). CrowdTangle نشان می‌دهد که این URL از زمان انتشار بیش از ۲۰ هزار واکنش، نظر و اشتراک‌گذاری در فیس‌بوک دریافت کرده است. همچنین برخی از صفحات و گروه‌های عمومی که پیوند را به اشتراک گذاشته‌اند را نشان می‌دهد و گزینه‌ای برای مشاهده‌ی داده‌های مشابه برای اینستاگرام، ردیت و توئیتر نیز ارائه می‌دهد. به یاد داشته باشید: در توئیتر فقط توئیت‌های هفت روز گذشته را خواهید دید.



توجه داشته باشید که تعداد واقعی کل تعاملات فیس‌بوک در این فهرست کوتاه صفحات و گروه‌ها بازتاب داده نشده است. این تا حدودی به این دلیل است که برخی از صفحات کلیدی‌ای که لینک را پس از اولین به‌اشتراک‌گذاری آن منتشر کردند، بعدتر توسط فیس‌بوک حذف شدند. خوب است به خاطر داشته باشید که CrowdTangle تنها داده‌های حساب‌های فعال را نشان می‌دهد و همه‌ی حساب‌های عمومی‌ای را که URL مشخصی را به اشتراک گذاشته‌اند نیز نشان نمی‌دهد. آنچه می‌بینید تنها گزیده‌ای از حساب‌هایی است که محتوا را به اشتراک گذاشته‌اند. اما همین میزان نیز بسیار مفید است، زیرا اغلب ارتباط واضحی بین حساب‌های کاربری خاص و یک وب‌سایت را نشان می‌دهد.

اگر یک صفحه‌ی فیس‌بوک به‌طور مداوم - یا منحصرا - محتوای سایت خاصی را به اشتراک بگذارد، می‌تواند نشان‌دهنده‌ی این باشد که هر دو توسط افراد مشابهی اداره می‌شوند. بنابراین می‌توانید از

صفحه‌ی فیس‌بوک برای جستجوهای بیشتر استفاده کنید و با مقایسه‌ی محتوای آن با وب‌سایت، راه‌هایی برای پیدا کردن افراد گرداننده و انگیزه‌های آن‌ها بیابید. برخی از نتایج اشتراک‌گذاری در فیس‌بوک نیز ممکن است افرادی را نشان دهند که لینک مورد نظر را در گروه‌های فیس‌بوک به اشتراک گذاشته‌اند. حساب کاربری‌ای که لینک را در گروه منتشر کرده پیدا کنید و ببینید آیا محتوای دیگری از وب‌سایت مورد نظر را نیز در گروه پست کرده است یا خیر. از این طریق نیز ممکن است موفق به کشف ارتباطات خاصی بین آن شخص و وب‌سایت مورد نظرتان بشوید.

ثبت دامنه

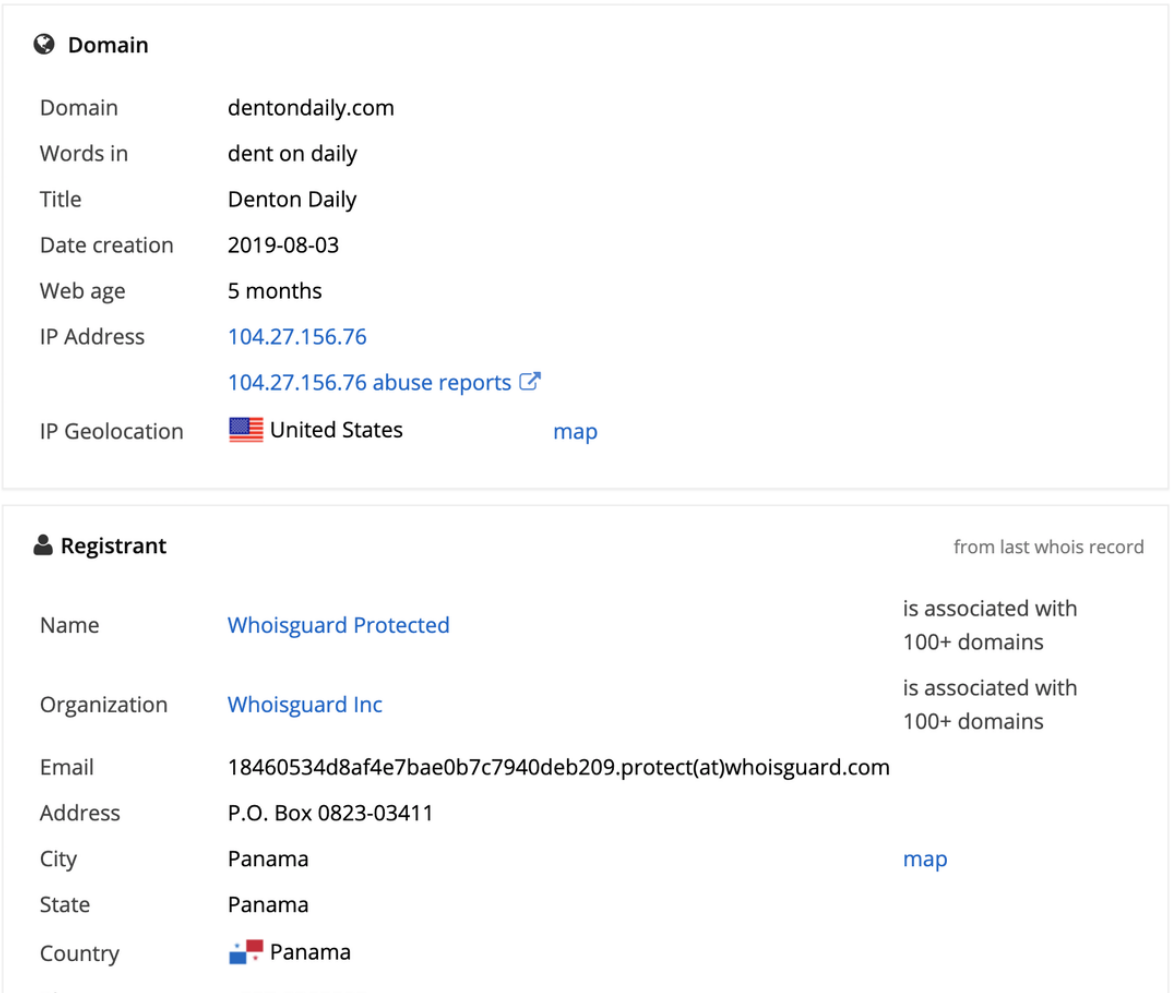
هر نام دامنه‌ای در فضای مجازی بخشی از یک پایگاه داده‌ی مرکزی است که اطلاعات اولیه در مورد ایجاد و تاریخچه‌ی آن را ذخیره می‌کند. در برخی موارد، اگر خوش‌شانس باشیم می‌توانیم اطلاعاتی نیز در مورد شخص یا نهادی که برای ثبت دامنه پول پرداخت کرده است، پیدا کنیم. این اطلاعات را می‌توانیم با جستجوی whois، که توسط بسیاری از ابزارهای رایگان ارائه می‌شود، به دست بیاوریم. همچنین، تعدادی ابزار عالی رایگان و یا ارزان نیز وجود دارد که می‌تواند اطلاعات بیشتری در اختیار شما قرار دهد، از جمله اینکه صاحبان دامنه در طول زمان چه کسانی بوده‌اند، سرورهایی که دامنه روی آن‌ها میزبانی شده و برخی جزئیات مفید دیگر.

یک نکته‌ی مهم این است که هنگام ثبت دامنه با پرداخت هزینه‌ای اندک می‌توان امکان محافظت از اطلاعات شخصی حریم خصوصی را فراهم کرد. اگر برای نام دامنه‌ای جستجوی whois انجام دهید و نتایج مواردی مانند "WhoisGuard Protected"، "Registration Private" یا "Perfect Privacy LLC" را نشان دهد به این معنی است که حریم خصوصی آن محافظت می‌شود. البته حتی در چنین مواردی نیز جستجوی whois همچنان تاریخ آخرین ثبت دامنه، زمان انقضای آن و آدرس IP جایی که دامنه میزبانی شده است را نشان خواهد داد.

DomainBigData یکی از بهترین ابزارهای رایگان برای بررسی نام دامنه و تاریخچه‌ی آن است. در این ابزار می‌توانید جستجوی خود را با نام شخص، شرکت یا حتی آدرس ایمیل به جای URL انجام دهید. سایر ابزارهای مقرون به صرفه‌ای که ممکن است به کارتان بیاید عبارتند از DNSlytics،

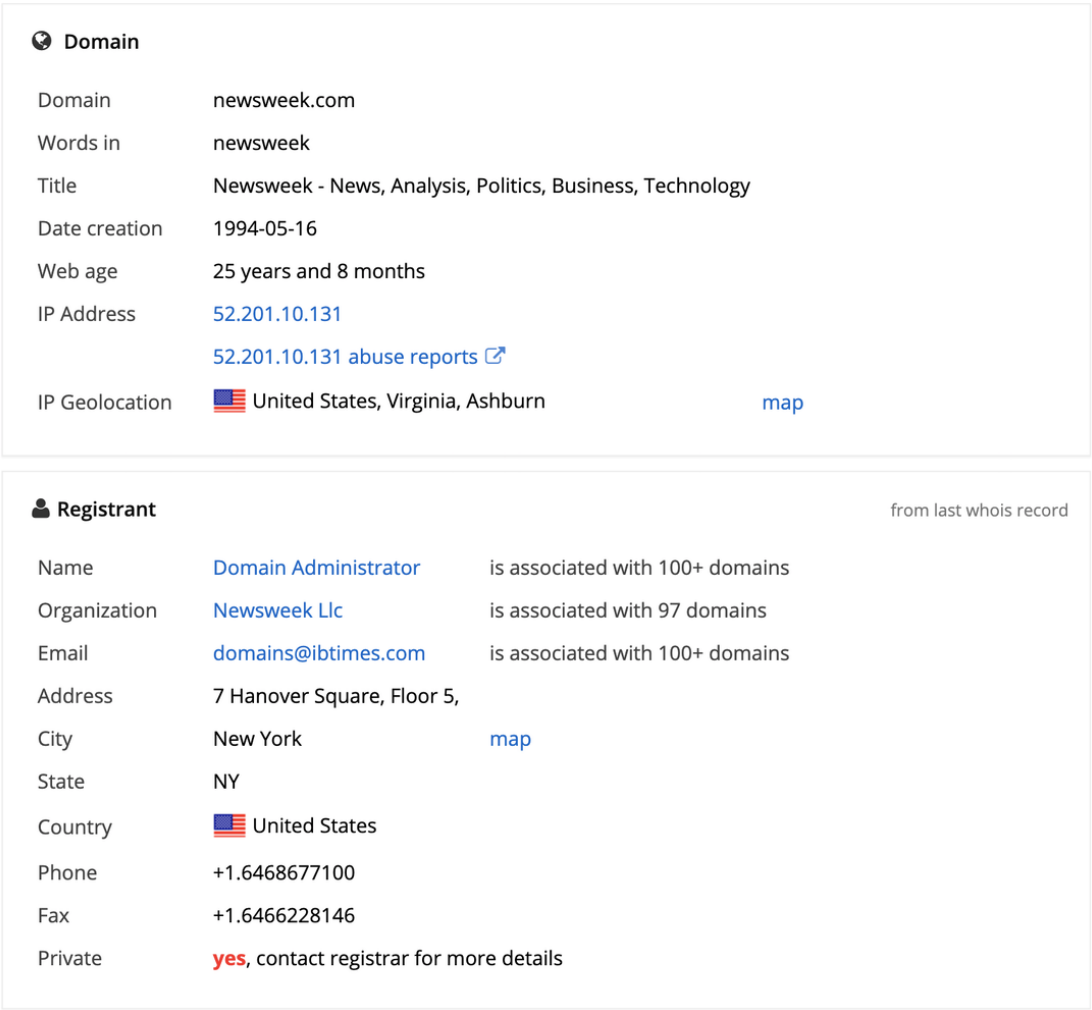
Security Trails و Whoisology.

یک گزینه‌ی گران‌تر اما عالی هم می‌تواند ابزار Iris investigations متعلق به DomainTools باشد. برای مثال، اگر dentondaily.com را در DomainBigData جستجو کنیم، خواهیم دید که ثبت‌کننده‌ی دامنه از گزینه‌ی محافظت از حریم خصوصی استفاده کرده و به جای نام ثبت‌کننده عبارت «Whoisguard Protected» را مشاهده خواهید کرد. خوشبختانه، هنوز هم می‌توانیم ببینیم که دامنه آخرین بار در آگوست ۲۰۱۹ ثبت شده است.



به‌عنوان مثالی دیگر، بیایید newsweek.com را در DomainBigData جستجو کنیم. بلافاصله

خواهیم دید که مالک برای حفاظت از حریم خصوصی پولی پرداخت نکرده است. نام شرکت، آدرس ایمیل، شماره تلفن و فکس شرکت موجود است.



Domain

Domain	newsweek.com
Words in	newsweek
Title	Newsweek - News, Analysis, Politics, Business, Technology
Date creation	1994-05-16
Web age	25 years and 8 months
IP Address	52.201.10.131
	52.201.10.131 abuse reports
IP Geolocation	United States, Virginia, Ashburn map

Registrant from last whois record

Name	Domain Administrator	is associated with 100+ domains
Organization	Newsweek Llc	is associated with 97 domains
Email	domains@ibtimes.com	is associated with 100+ domains
Address	7 Hanover Square, Floor 5,	
City	New York	map
State	NY	
Country	United States	
Phone	+1.6468677100	
Fax	+1.6466228146	
Private	yes, contact registrar for more details	

همچنین می‌بینیم که این نهاد از ماه مه ۱۹۹۴ مالک دامنه است و این سایت در حال حاضر در آدرس IP 52.201.10.13 میزبانی می‌شود. نکته‌ی بعدی‌ای که باید به آن توجه کنید این است که نام شرکت، ایمیل و آدرس IP همه به شکل لینک برجسته شده‌اند. این یعنی با کلیک کردن روی آن‌ها به دامنه‌های دیگری که متعلق به domains@ibtimes.com ،Newsweek LLC و سایر وب‌سایت‌هایی است که در همان آدرس IP میزبانی می‌شوند هدایت خواهید شد. این ارتباطات در

تحقیقات بسیار مهم هستند، بنابراین همیشه باید به سایر دامنه‌های متعلق به یک شخص یا نهاد دقت کنید.

در مورد آدرس‌های IP دقت داشته باشید که وب‌سایت‌هایی که هیچ اتصالی با هم ندارند ممکن است روی سرور یکسانی میزبانی شوند. دلیل آن این است که افراد اغلب از یک شرکت میزبان برای تمام وب‌سایت‌های خود استفاده می‌کنند. یک قانون کلی این است که هر چه تعداد وب‌سایت‌های میزبانی‌شده روی یک سرور کمتر باشد، احتمال ارتباط آن‌ها با هم بیشتر می‌شود. اما این یک قانون قطعی نیست.

اگر صدها سایت روی یک سرور میزبانی شده باشند، این احتمال وجود دارد که هیچ ارتباطی بین مالکان آن‌ها وجود نداشته باشد. اما برای مثال، اگر فقط ۹ دامنه روی سرور میزبان ثبت شده و اطلاعات ثبت دامنه‌ی وب‌سایت مورد نظر شما هم خصوصی است، ارزش آن را دارد که برای ۸ دامنه‌ی دیگر جستجوی whois انجام دهید تا ببینید آیا مالکشان یکسان است یا خیر، و آیا این امکان وجود دارد آن شخص همچنین مالک سایتی باشد که شما در حال بررسی‌اش هستید؟ افراد ممکن است برای حفاظت از حریم خصوصی بعضی از دامنه‌ها هزینه کنند اما از انجام آن برای دیگر دامنه‌های متعلق به خود غافل شوند.

شناسایی ارتباط بین وب‌سایت‌ها با استفاده از آدرس IP، محتوا و/یا اطلاعات ثبت‌نام راهی بسیار مهم برای شناسایی شبکه‌ها و عواملی است که پشت این شبکه‌ها هستند و آن‌ها را اداره می‌کنند.

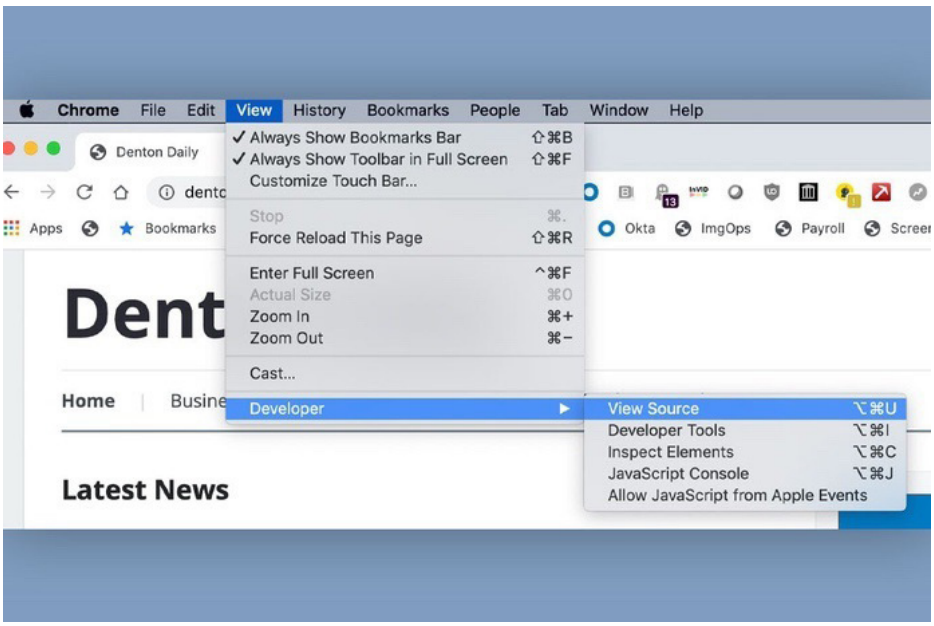
حالا می‌رویم به سراغ بررسی راهی دیگر برای شناسایی ارتباط وب‌سایت‌ها با هم با استفاده از کد صفحه‌ی وب.

کد و تجزیه و تحلیل

این روش اولین بار توسط لارنس الکساندر ابداع شد و با مشاهده‌ی کد منبع یک صفحه‌ی وب و سپس جستجو در آن برای پیدا کردن کد گوگل آنالتیکس و/یا گوگل ادسِنس، شروع می‌شود. این‌ها محصولات بسیار محبوب گوگل هستند که به‌ترتیب به صاحب سایت این امکان را می‌دهند که آمار

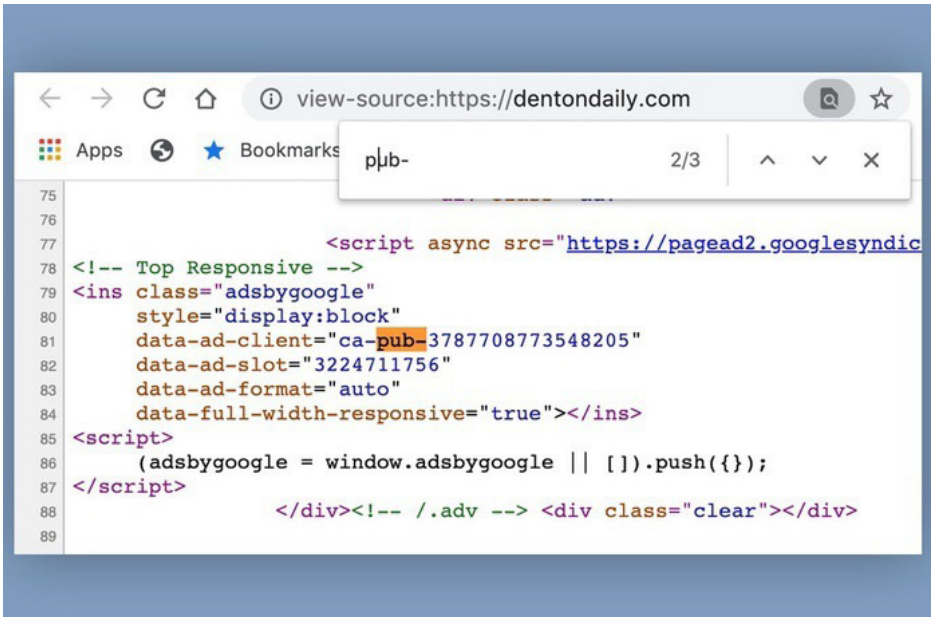
وب‌سایت را ردیابی کرده یا از طریق تبلیغات کسب درآمد کند. پس از جایگذاری در یک سایت، هر صفحه‌ی وب یک شناسه‌ی منحصربه‌فرد خواهد داشت که به حساب آنالتیکس یا ادسنس مالک مرتبط است. اگر شخصی چندین سایت داشته باشد، اغلب از یک حساب آنالتیکس یا ادسنس برای مدیریت آن‌ها استفاده می‌کند. این فرصتی برای محقق فراهم می‌کند که با پیدا کردن شناسه‌ی یکسان در کد منبع، ارتباط بین سایت‌های به ظاهر مجزا را پیدا کند. خوشبختانه، انجام این کار آسان است.

ابتدا به وب‌سایت مورد نظر خود بروید. اجازه بدهید برای مثال از dentondaily.com استفاده کنیم. در نسخه‌ی Google Chrome که برای Mac طراحی شده، ابتدا به منوی View بروید و سپس Developer و درنهایت View Source را انتخاب کنید. با این کار یک تب جدید با کد منبع صفحه باز می‌شود (در نسخه‌ی Chrome برای رایانه‌های شخصی، ctrl- U را فشار دهید).

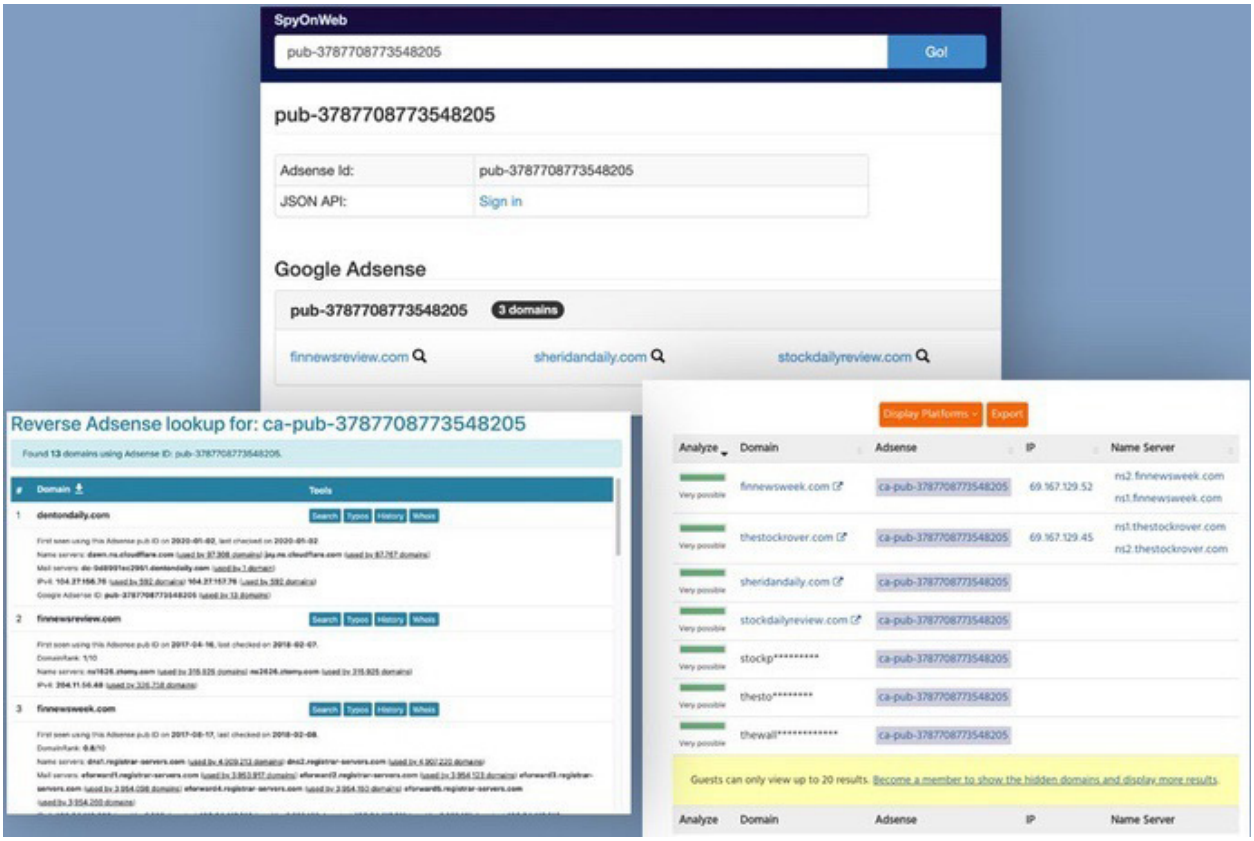


همه‌ی شناسه‌های گوگل آنالتیکس با «ua-» شروع می‌شوند و به دنبال آن یک رشته اعداد می‌آیند. شناسه‌های ادسنس دارای «pub-» و یک رشته اعداد هستند. می‌توانید با انجام یک جستجوی ساده

در صفحه، این شناسه‌ها را در کد منبع پیدا کنید. در Mac، Command-F را بگیرید و در کامپیوترهای دیگر ctrl-F. با این کار یک کادر جستجوی کوچک ظاهر می‌شود. پیشوندهای شناسه را وارد کنید و سپس هر شناسه‌ای که در کد منبع صفحه موجود باشد را مشاهده خواهید کرد.



اگر شناسه‌ای پیدا کردید، آن را کپی کرده و در کادر جستجوی سرویس‌هایی مانند، SpyOnWeb، NerdyData، DNSlytics یا AnalyzeID واردش کنید. توجه داشته باشید که اغلب نتایج متفاوتی از هر سرویس دریافت می‌کنید، بنابراین مهم است که یک شناسه را با ابزارهای مختلف بررسی و نتایج را با هم مقایسه کنید. در تصویر زیر، می‌توانید مشاهده کنید که SpyOnWeb سه دامنه با شناسه‌ی ادسنس مورد نظر پیدا کرده است، اما DNSlytics و AnalyzeID چندین دامنه دیگر نیز پیدا کرده‌اند.



گاهی اوقات سایتی که در گذشته یک شناسه داشته، دیگر وجود ندارد. به همین دلیل ضروری است که از همان رویکرد مشاهده‌ی کد منبع برای تمام سایت‌های دیگری که شناسه‌ی مورد نظر برای آن‌ها نشان داده شده استفاده کنید تا مطمئن شوید این سایت‌ها هنوز وجود دارند. توجه داشته باشید که اگر وب‌سایت حذف شده باشد شناسه‌های ادسنس و آنالتیکس آن هنوز در نسخه‌ی بایگانی‌شده‌اش در Wayback Machine وجود دارند. بنابراین اگر در کد منبع یک سایت موجود شناسه‌ای پیدا نکردید، جستجوی خود را در Wayback Machine تکرار کنید.

همه‌ی این ابزارها بخشی از نتایج را به صورت رایگان ارائه می‌دهند. اما اغلب برای دریافت نتایج کامل باید هزینه پرداخت کنید، به خصوص اگر شناسه‌ی مورد نظر شما در تعداد زیادی از سایت‌های دیگر موجود باشد.

یک نکته‌ی آخر در مورد بازرسی کد منبع: حتی اگر با PHP، JavaScript، HTML یا سایر زبان‌های رایج برنامه‌نویسی وب آشنایی ندارید، ارزش آن را دارد که کل صفحه را بررسی کنید. به‌عنوان مثال، گاهی اوقات افراد در صورت استفاده‌ی مجدد از قالب‌های آماده برای طراحی وب‌سایت ، فراموش می‌کنند که عنوان یک صفحه یا وب‌سایت را تغییر دهند. این خطای ساده می‌تواند همان نقطه‌ی اتصال مورد نظرتان باشد.

در حین بررسی کلاه‌برداری تبلیغات دیجیتال که شرکت‌های صوری‌ای مانند آتوسس داشت، در حال بررسی شرکتی به نام فلای اَپس بودم. وقتی به کد منبع این وب‌سایت یک صفحه‌ای نگاه کردم، جایی نزدیک بالای کد سایت کلمه‌ی“Loocrum” به وضوح دیده می‌شد:

این نام را در گوگل جستجو کردم و شرکتی به نام Loocrum را پیدا کردم که از قالب طراحی‌ای درست شبیه به سایت فلای اپس استفاده کرده بود و محتوایی مشابه آن نیز داشت. جستجوی whois نشان داد که آدرس ایمیل مورد استفاده برای ثبت loocrum.com برای ثبت شرکت‌های صوری دیگری که قبلا در این طرح شناسایی کرده بودم نیز استفاده شده است. این ارتباط بین فلای اپس و لوکروم

شواهد مهمی را ارائه داد که نشان می‌داد چهار مردی که فلای اپس را اداره می‌کردند با این طرح بزرگ کلاهبرداری مرتبط بودند؛ شواهدی که با جستجوی ساده‌ی کد منبع و گشتن به دنبال کلماتی که با باقی کد بی‌ارتباط به نظر می‌رسیدند به دست آمده بود.

نتیجه‌گیری

حتی با وجود تمام روش‌ها و ابزارهای بالا، ممکن است گاهی اوقات احساس کنید که به بن‌بست رسیده‌اید. اما اغلب راه دیگری برای پیدا کردن ارتباطات یا راه‌هایی برای بررسی بیشتر در یک وب‌سایت وجود دارد. روی تمام لینک‌ها کلیک کنید، محتوای سایت را مطالعه کنید، کد منبع آن را بخوانید، میزبان دامنه‌ی آن را پیدا کنید، ببینید چه کسی مطالب آن را به اشتراک می‌گذارد، و هر چیز دیگری را که به فکرتان می‌رسد بررسی کنید تا نشان دهید واقعاً چه خبر است.

۹. تجزیه و تحلیل تبلیغات در شبکه‌های اجتماعی

نوشته‌ی: **جوانا وایلد**

جوانا وایلد محقق داده‌های منبع‌باز در بلینگ‌کت است. او همچنین بر توسعه‌ی فناوری و ابزار برای تحقیقات دیجیتال نیز تمرکز دارد. او سابقه‌ی روزنامه‌نگاری آنلاین را نیز دارد و پیش از این در مناطق (پسا)درگیری با روزنامه‌نگاران کار کرده است. یکی از نقش‌های او حمایت از روزنامه‌نگاران در شرق آفریقا برای تولید برنامه جهت پخش در صدای آمریکا بود.

تبلیغاتی که شما در تایم‌لاین رسانه‌های اجتماعی خود می‌بینید با آنچه افرادی که در وسایل حمل و نقل عمومی در کنار شما نشسته‌اند می‌بینند یکسان نیست. بر اساس عواملی مانند موقعیت مکانی، جنسیت، سن و چیزهایی که در شبکه به اشتراک گذاشته و یا لایک کرده‌اید، ممکن است تبلیغات یک تعطیلات مجلل در مالاگا به شما نشان داده شود در حالیکه همسایه‌ی شما تبلیغات بازی‌های تلفن همراه ژاپنی را می‌بیند.

در زمان انتخابات هدف‌گذاری مبتنی بر فرد (میکروتارگتینگ)، که کاربران را به گروه‌های هدف مجزا تقسیم کرده و به هر گروهْ تبلیغاتی منطبق با شرایط زندگی و علایقشان را نشان می‌دهد، به یکی از نگرانی‌های اصلی تبدیل شده است. نگرانی عمده این است که کمپین‌ها می‌توانند بخش‌های بسیار کوچکی از جمعیت را با تبلیغاتی که ترس یا نفرت را در آنها برمی‌انگیزد یا اطلاعات نادرست در اختیارشان قرار می‌دهد هدف قرار دهند. به‌طور کلی، تبلیغاتی که توسط سیاستمداران در شبکه‌های اجتماعی به اشتراک گذاشته می‌شود مورد راستی‌آزمایی قرار نمی‌گیرد. به‌عنوان مثال، فیس‌بوک در ژانویه‌ی ۲۰۲۰ یک بار دیگر اعلام کرد به اشتراک گذاشتن تبلیغات سیاسی، مادامی که با استانداردهای این شبکه‌ی اجتماعی مغایرت نداشته باشد، مانعی ندارد. این بدان معناست که گروه‌های خاصی از کاربران ممکن است با تبلیغاتی که حاوی اطلاعات نادرست درباره‌ی موضوعات مهم سیاسی یا اجتماعی هستند هدف قرار گیرند.

تا همین اواخر، به دست آوردن هرگونه اطلاعات و بینشی درباره‌ی تبلیغاتی که برای کاربران مختلف

هدف‌گذاری شده بود برای روزنامه‌نگاران و محققین تقریبا غیرممکن بود. در پاسخ به انتقاد عمومی در مورد عدم شفافیت، چندین شبکه‌ی اجتماعی اقدام به ایجاد کتابخانه‌های تبلیغات کردند که به هر کسی اجازه می‌دهد اطلاعات مربوط به تبلیغات منتشرشده در پلتفرم را بررسی کند.

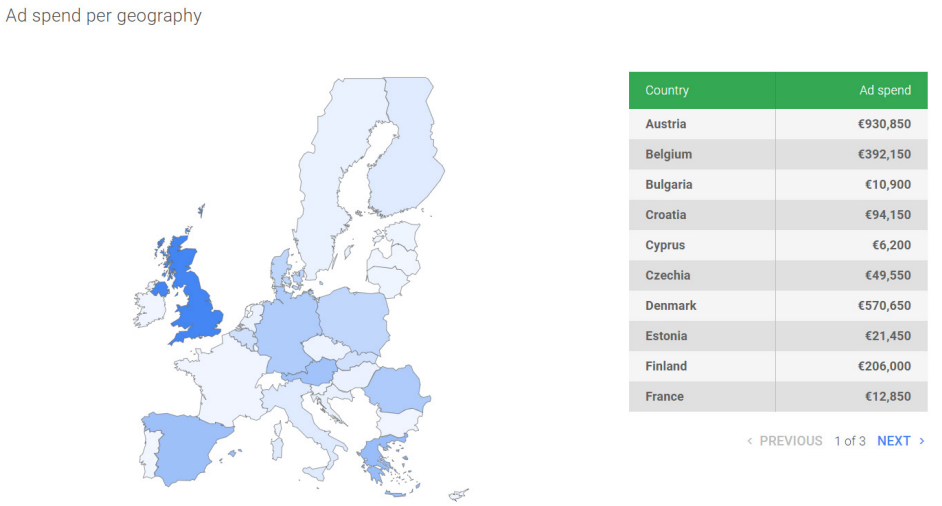
از این میان، کتابخانه‌ی فیس‌بوک به‌طور اخص متهم شده است که همه‌ی تبلیغات موجود در پلتفرم را در کتابخانه نشان نمی‌دهد. بنابراین، هر زمان که از این کتابخانه‌ها استفاده می‌کنید، کمی وقت بگذارید و بررسی کنید که آیا همه‌ی تبلیغاتی که در تایم‌لاین خود می‌بینید را می‌توانید در آنجا پیدا کنید یا خیر.

بااین‌حال، کتابخانه‌های تبلیغات گام مهمی به سوی شفافیت بیشتر هستند و راه‌های جدید و جالبی برای بررسی تبلیغات دیجیتال در اختیار روزنامه‌نگاران و دیگران قرار می‌دهند. تکنیک‌های زیر به شما کمک خواهند کرد تحقیقات خود را در مورد تبلیغاتی که در پلتفرم‌های اصلی مانند گوگل، توئیتر و فیس‌بوک منتشر می‌شوند شروع کنید.

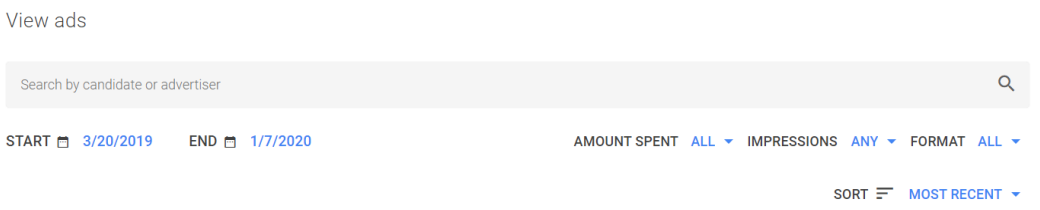
گوگل

مرکز تبلیغات گوگل به‌خوبی در گزارش شفافیت آن پنهان شده است. از این لینک برای دسترسی به بخش تبلیغات سیاسی استفاده کنید، که اطلاعاتی در مورد تبلیغات گوگل و یوتیوب از اتحادیه اروپا، هند و ایالات متحده ارائه می‌دهد.

صفحه‌ی هر منطقه فهرستی از کشورها و کل هزینه‌ی تبلیغات را از زمان راه‌اندازی این گزارش نشان می‌دهد.



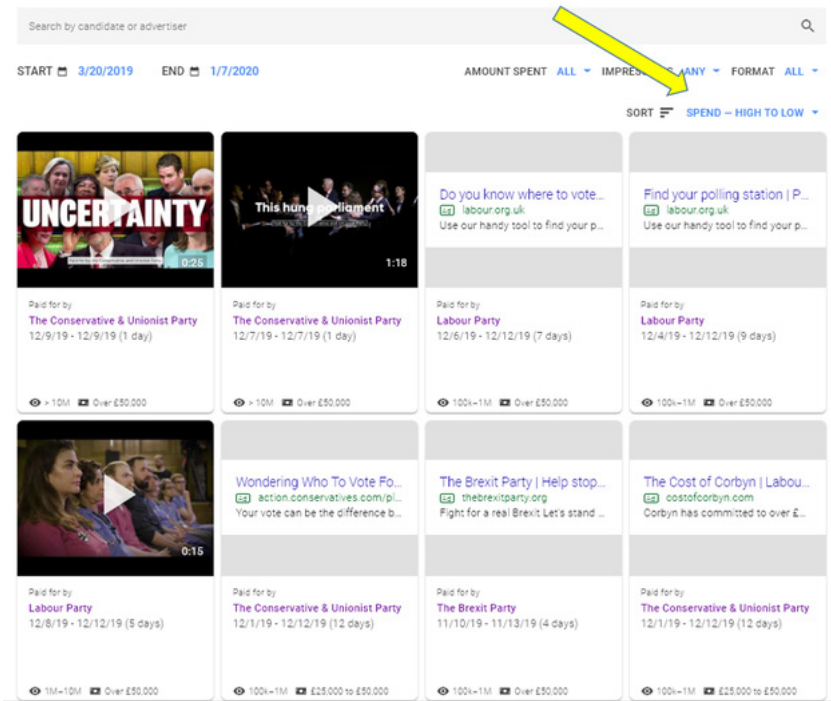
با کلیک کردن بر روی هر کشور، به صفحه‌ی حاوی پایگاه داده‌ی تبلیغات آن هدایت خواهید شد:



می‌توانید نتایج را بر اساس تاریخ، مقدار هزینه‌ی صرف‌شده و تعداد دفعاتی که یک تبلیغ به کاربران نشان داده می‌شود (نمایش‌ها) فیلتر کنید. اگر می‌خواهید نتایج مربوط به تبلیغات ویدئویی، تصویری

یا متنی را مشاهده کنید، می‌توانید نتایج را بر اساس فرمت تبلیغات فیلتر کنید.

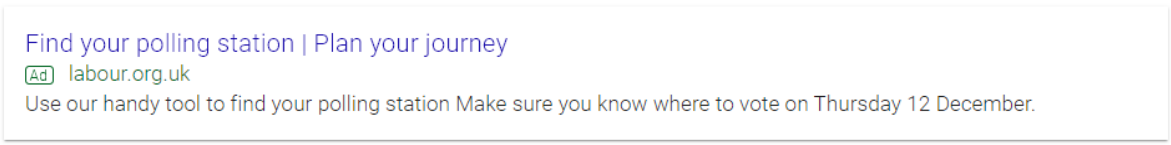
همچنین، پیدا کردن افراد و نهادهایی که بیشترین هزینه را صرف تبلیغات کرده‌اند نیز بسیار ساده است. به‌عنوان مثال، اگر می‌خواهید بزرگترین کمپین‌های تبلیغات سیاسی در بریتانیا از زمان انتشار گزارش تا ژانویه ۲۰۲۰ را مشاهده کنید، همانطور که در زیر نشان داده شده است به‌سادگی طبقه‌بندی «Sort» را به «spend high to low» تغییر دهید.



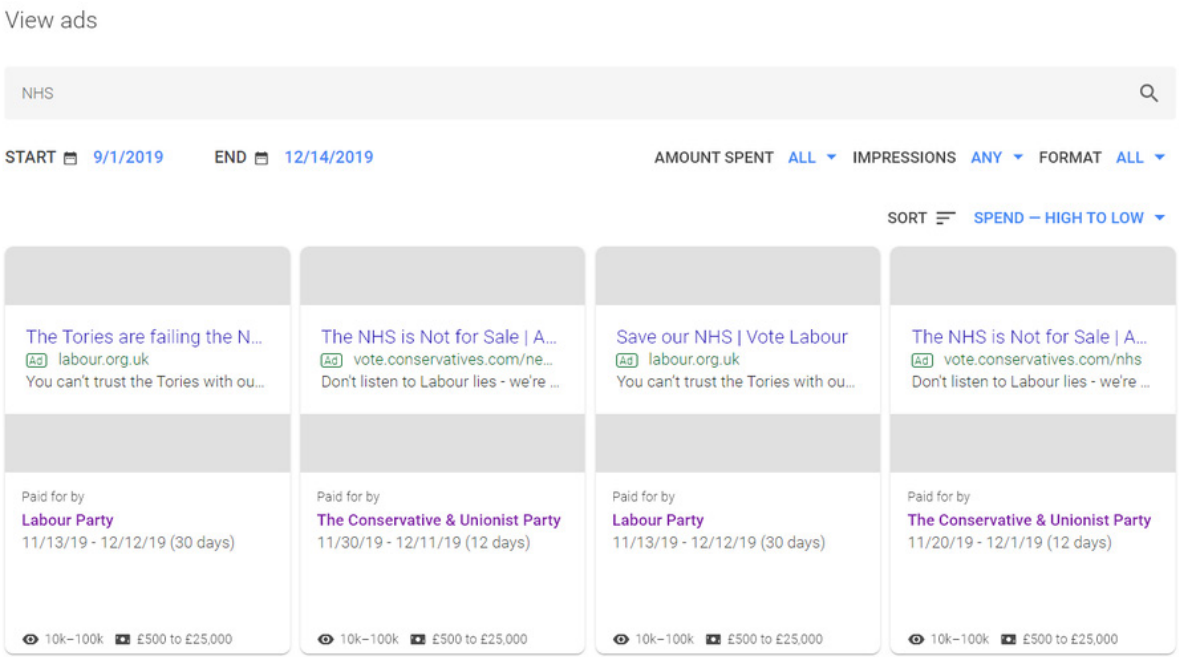
جای تعجب نیست که بیشترین خرید تبلیغات درست روز قبل از انتخابات و در روز انتخابات عمومی، یعنی ۱۲ دسامبر ۲۰۱۹ صورت گرفته است. همچنین، می‌توانید ببینید که احزاب محافظه‌کار و اتحادگرا هر کدام بیش از ۵۰ هزار پوند برای دو آگهی تبلیغاتی در یوتیوب که فقط به‌مدت یک روز پخش شدند، هزینه کرده‌اند.

در مقابل، حزب کارگر بیش از ۵۰ هزار پوند برای تبلیغ در صفحات نتایج جستجوی گوگل برای تبلیغ

ابزاری هزینه کرده که به گفته‌ی آن می‌تواند به رأی‌دهندگان کمک کند پایگاه رأی‌دهی نزدیک به خود را پیدا کنند.

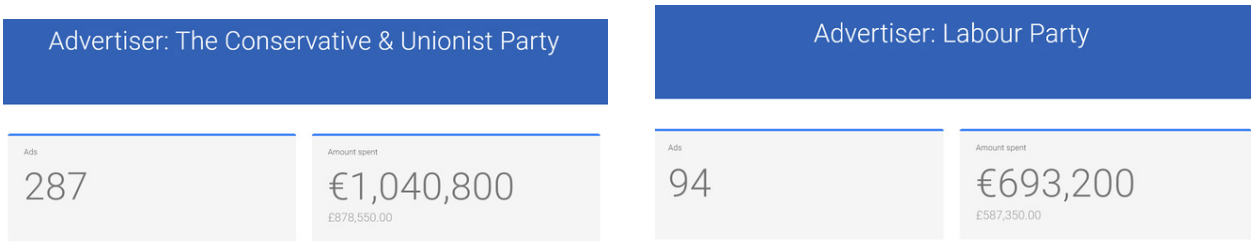


همچنین می‌توانید جستجوی خود را با یک کلمه‌ی کلیدی انجام دهید. NHS (مخفف سرویس سلامت همگانی) را تایپ کنید و خواهید دید که در نوامبر و دسامبر ۲۰۱۹، حزب کارگر و محافظه‌کار تبلیغات جستجوی گوگل را خریداری کرده‌اند تا از برنامه‌های یکدیگر برای سرویس سلامت همگانی انتقاد کنند.



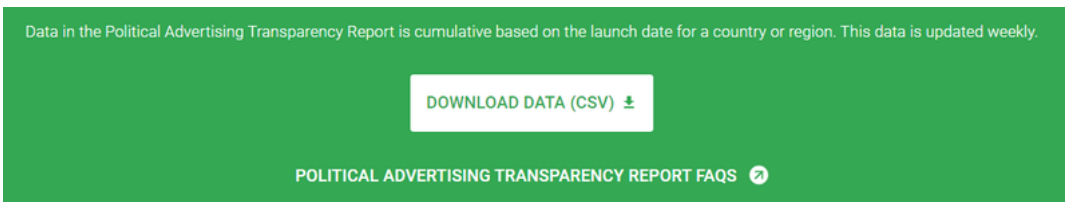
همچنین، با کلیک روی نام تبلیغ‌کننده می‌توانید کل مبلغی را که از زمان راه‌اندازی گزارش شفاف‌سازی برای تبلیغات گوگل خرج کرده‌اند، بررسی کنید. وضعیت برای دو حزب سیاسی مهم بریتانیا در ژانویه‌ی

۲۰۲۰ به شکل زیر بود:



به‌علاوه، می‌توانید جدول زمانی هزینه‌های آن‌ها را نیز مشاهده کنید. گزارش‌های سمت چپ الگوی هزینه‌های احزاب محافظه‌کار و اتحادگرا، و گزارش سمت راست الگوی مربوط به حزب کارگر را نشان می‌دهند:

اگر می‌خواهید پایگاه داده‌ی تبلیغات را بیشتر تجزیه و تحلیل کنید، به پایین صفحه بروید تا بخش سبزرنگی با عنوان «DOWNLOAD DATA» را مشاهده کنید که به شما امکان می‌دهد داده‌ها را در قالب CSV دانلود کنید.



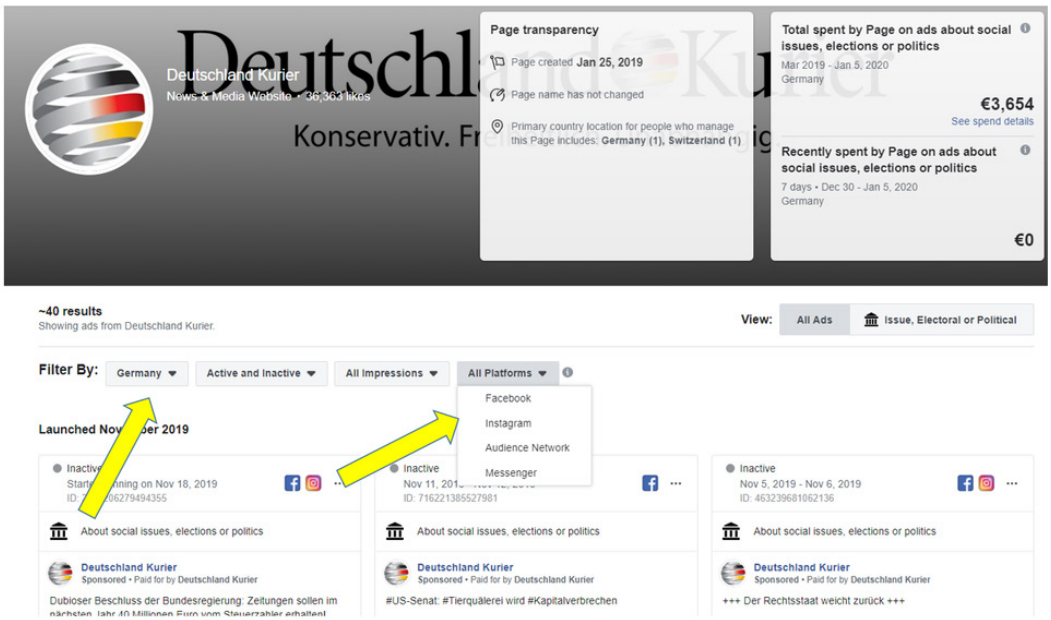
به‌این‌ترتیب می‌توانید داده‌ها را به یک برنامه‌ی صفحه گسترده مانند Google Sheets یا Excel وارد کنید تا بتوانید آن‌ها را غربال کرده و تجزیه و تحلیل بیشتری روی داده‌ها انجام دهید.

فیس‌بوک

کتابخانه‌ی تبلیغات فیس‌بوک به دو بخش تقسیم می‌شود: «همه‌ی تبلیغات» (All Ads) و «مسائل اجتماعی، انتخاباتی یا سیاسی» (Issue, Electoral or Political) . اگر روی «همه‌ی تبلیغات» کلیک کنید، می‌توانید به جای استفاده از کلمات کلیدی، تبلیغ‌کنندگان خاص را فقط با نام جستجو کنید.

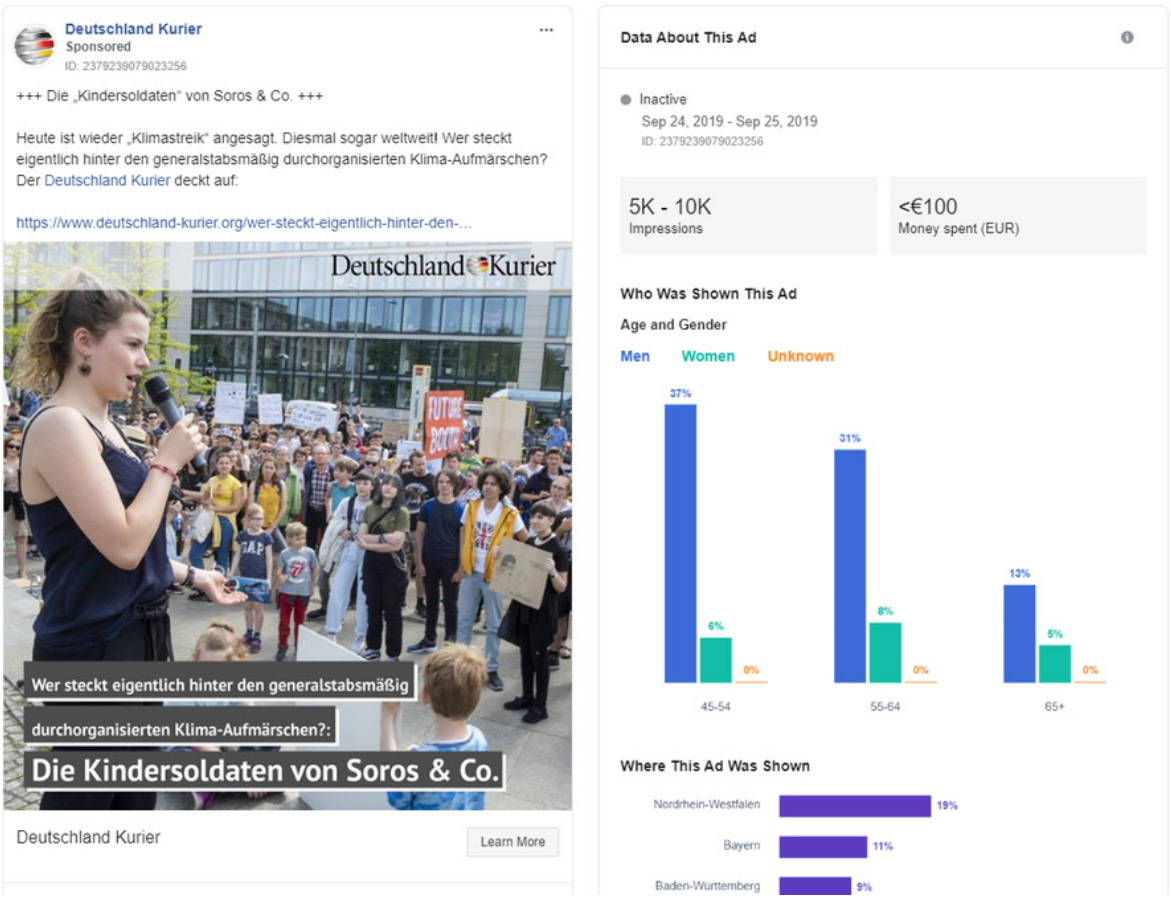
برای مثال، اگر بخواهم تبلیغات Deutschland Kurier، نشریه‌ای که اغلب مطالبی در حمایت از حزب راست افراطی آلترناتیو برای آلمان (AfD) منتشر می‌کند، را مشاهده کنم می‌توانم نام آن را تایپ کنم و فیس‌بوک صفحاتی با آن نام را نشان خواهد داد:

نتایج نشان می‌دهد که Deutschland Kurier بین مارس ۲۰۱۹ و ژانویه‌ی ۲۰۲۰ تبلیغاتی به ارزش ۳۶۵۴ یورو در آلمان انجام داده است.



مطمئن شوید در صفحه‌ی نتایج کشور صحیح (یا گزینه‌ی All) را برای جستجوی خود انتخاب کرده‌اید. به‌علاوه، در این صفحه می‌توانید انتخاب کنید که آیا می‌خواهید تبلیغات از فیس‌بوک، اینستاگرام، مسنجر یا شبکه‌ی مخاطبان فیس‌بوک به شما نشان داده شود. شبکه‌ی مخاطبان فیس‌بوک (Audience Network) یک شبکه‌ی تبلیغاتی است که توسط فیس‌بوک اداره می‌شود و تبلیغات را در برنامه‌های تلفن همراه و وب‌سایت‌هایی غیر از آن‌هایی که در مالکیت خود فیس‌بوک هستند نیز قرار می‌دهد. در بیشتر موارد، بهترین انتخاب جستجو در همه‌ی پلتفرم‌ها برای دریافت تصویری کامل از تبلیغات یک سازمان است.

برای هر آگهی می‌توانید روی گزینه‌ی «See ad details» کلیک کنید تا اطلاعات اضافی درباره‌ی آن را مشاهده کنید.

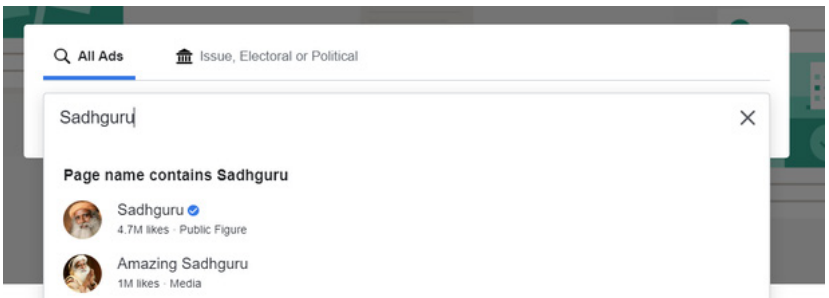


در این مورد، Deutschland Kurier کمتر از ۱۰۰ یورو برای آگهی‌ای هزینه کرده است که معترضان تغییرات آب‌وهوایی را «کودک‌سربازان سوروس و شرکاء» می‌نامد، و بین ۵ تا ۱۰ هزار بار، و عمدتا برای مردان ۴۵ سال به بالا، نمایش داده شده است.

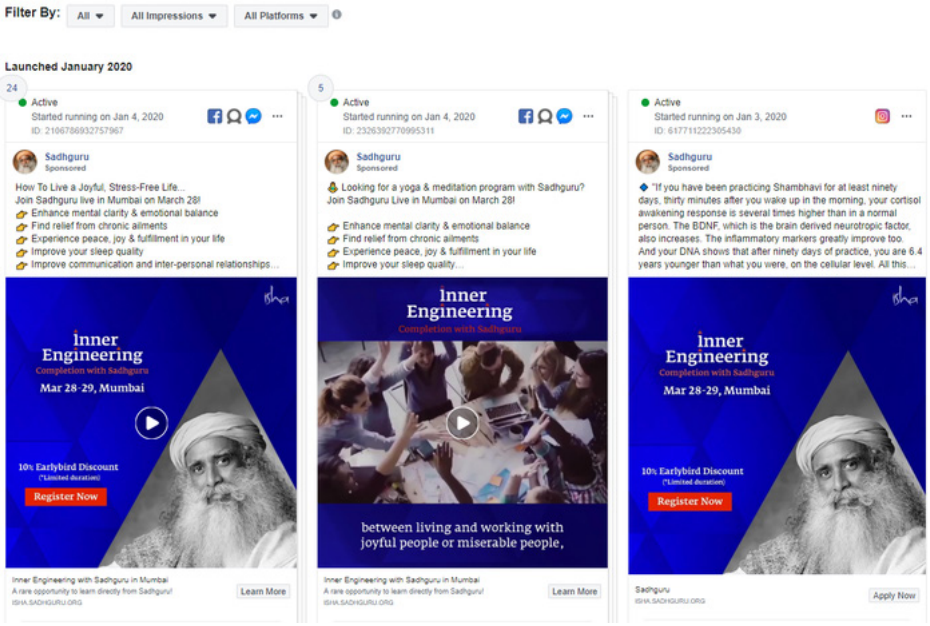
گزینه‌ی دوم برای جستجوی کتابخانه تبلیغات، انتخاب پایگاه داده «Issue, Electoral or Political» است که آرشیو تبلیغاتی درباره‌ی «مسائل اجتماعی، انتخابات یا سیاست» است. مزیت بزرگ این گزینه این است که می‌توانید هر کلمه‌ی کلیدی‌ای را که دوست دارید جستجو کنید و این نوع تبلیغات توسط فیس‌بوک آرشیو می‌شوند.

بیایید با هم نگاهی به یک مثال بیندازیم.

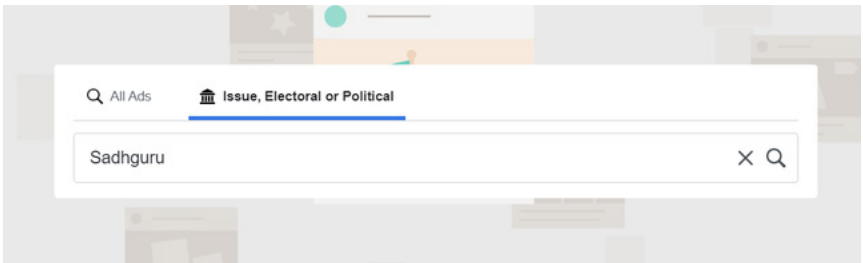
سادگورو نام یک روحانی معروف هندی است؛ عارفی که می‌گوید با هیچ حزب سیاسی‌ای مرتبط نیست. او گفته است که وظیفه‌ی خود می‌داند از هر دولتی که بر سر کار باشد حمایت کند «تا کار خود را به بهترین وجه ممکن انجام دهد». اگر نام او را در بخش «همه‌ی تبلیغات» تایپ کنید، فیس‌بوک صفحه‌ی شخصی سادگورو را پیشنهاد می‌کند.



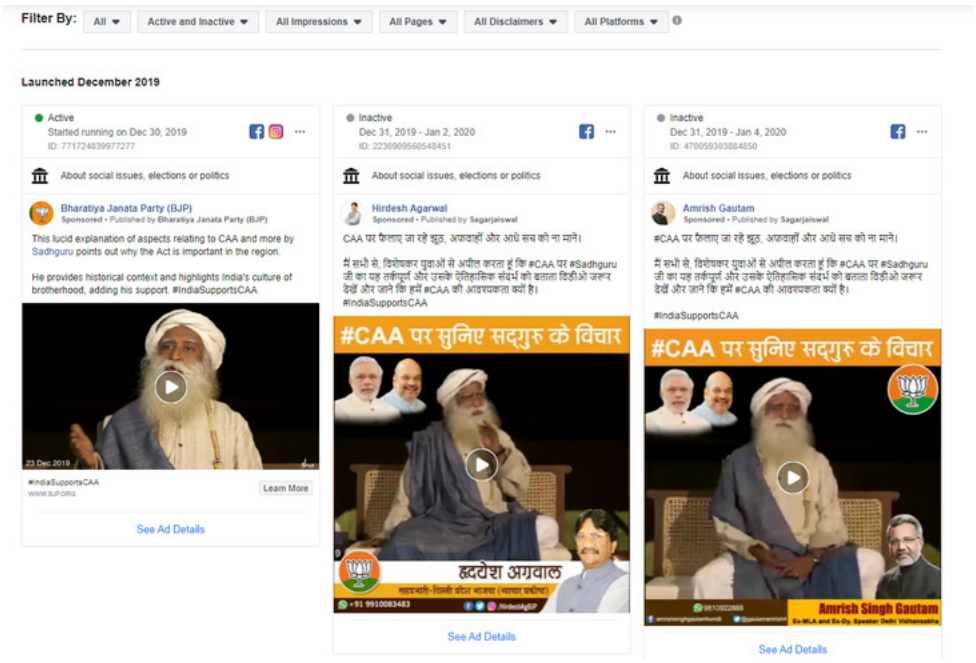
نتایج این جستجو تبلیغات غیرسیاسی‌ای را نشان می‌دهند که بیشتر به دوره‌های آموزشی یوگا و مدیتیشن که توسط سادگورو برگزار می‌شود اختصاص دارند.



حالا اجازه بدهید به جای پذیرفتن چیزهایی که فیس‌بوک برای ما انتخاب و آن‌ها را در نتایج فهرست کرده است، نام سادگورو را در دسته‌ی دیگر تبلیغات، یعنی تبلیغات مربوط به مسائل اجتماعی، سیاسی و انتخاباتی جستجو کنیم:



نتایج به‌شدت تغییر می‌کنند. این بار مجموعه‌ای از تبلیغات را مشاهده می‌کنید که توسط صفحات دیگر منتشر شده و نام سادگورو در آن‌ها ذکر شده است.



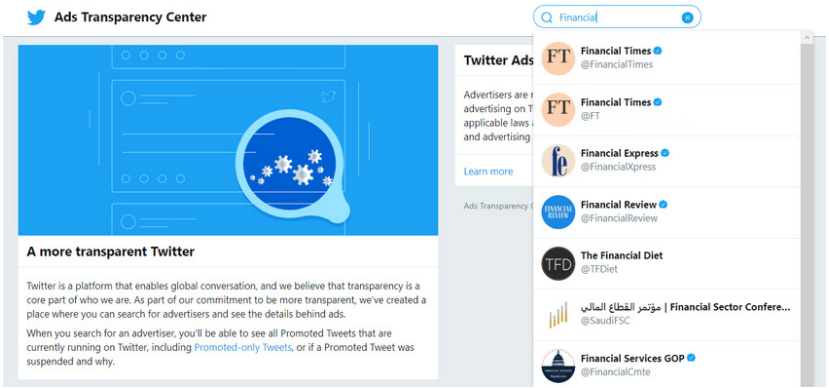
یکی از تبلیغات حزب ملی‌گرای هند موسوم به حزب بهاراتیا جاناتا (BJP) ویدئویی را نشان می‌دهد که در آن سادگورو حمایت خود را از لایحه‌ی بحث‌برانگیز اصلاح موادی از حقوق شهروندی که توسط این حزب ارائه شده اعلام می‌کند. این لایحه به مهاجران ثبت‌نشده از برخی از کشورهای همسایه‌ی هند اجازه می‌دهد راحت‌تر به تابعیت هندی دست پیدا کنند، اما این امتیاز را به مسلمانان نمی‌دهد. این آگهی اشاره‌ای ضمنی به رابطه‌ی احتمالی بین سادگورو و بی‌جی‌پی دارد ، موضوعی که به‌طور گسترده در هند مورد بحث قرار گرفته است.

این مثال نشان می‌دهد که چگونه می‌توانید از کتابخانه‌ی تبلیغات فیس‌بوک برای افزودن اطلاعات کلیدی به تحقیقات خود استفاده کنید. همچنین می‌توانید به گزارش کتابخانه‌ی تبلیغات فیس‌بوک نیز نگاهی بیندازید که حاوی بینش‌های کلیدی از تبلیغات سیاسی در کشورهای مختلف است.

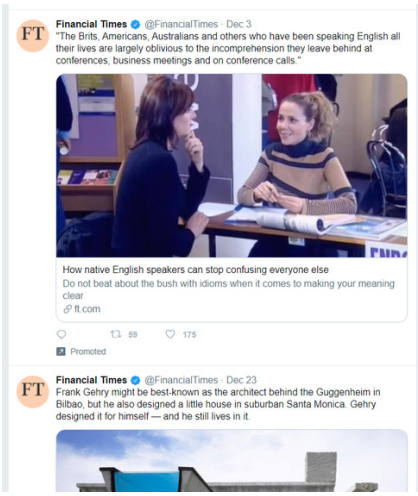
توئیتر

اواخر سال ۲۰۱۹، توئیتر تصمیم گرفت تبلیغات سیاسی را در پلتفرم خود ممنوع کند. بااین‌حال، هنوز هم می‌توان از مرکز شفافیت تبلیغات این شبکه‌ی اجتماعی برای کسب اطلاعات درباره‌ی تبلیغات غیرسیاسی ۷ روز گذشته استفاده کرد.

پیدا کردن تبلیغات در توئیتر دشوار است، زیرا هیچ قابلیتی برای جستجوی کلمه‌ی کلیدی وجود ندارد. برای شروع جستجو، به کادر گوشه‌ی بالا سمت راست بروید و یک نام کاربری خاص را تایپ کنید.



اگر طی ۷ روز گذشته تبلیغاتی وجود داشته باشد، آن‌ها را در فهرست خواهید دید.



با جستجوی فایننشال تایمز، می‌توانیم ببینیم که این کاربر برای جلب توجه بیشتر به یکی از مطالب خود، مقاله‌ای با عنوان «چگونه انگلیسی‌زبانان می‌توانند بقیه‌ی کسانی را که از این زبان استفاده می‌کنند گیج نکنند»، هزینه‌ای را پرداخت کرده است. این توئیت در تاریخ ۳ دسامبر ۲۰۱۹ ارسال شده است، اما اطلاعات تبلیغاتی توئیتر جزئیات دقیقی در مورد زمان اجرای این تبلیغات پولی ارائه نمی‌دهد.

برای سرعت بخشیدن به جستجوی خود، می‌توانید از یک ترفند کوچک استفاده کنید. پس از انجام جستجو، به URL موجود در مرورگرتان نگاهی بیندازید:

```
ads.twitter.com/transparency/FinancialTimes
```

URL همیشه از ساختار یکسانی استفاده می‌کند که نام کاربری توئیتر در انتهای آن قرار دارد. بنابراین می‌توانید به‌سادگی قسمت آخر را حذف کرده و با یک نام کاربری دیگر جایگزینش کنید:

```
ads.twitter.com/transparency/Bellingcat
```

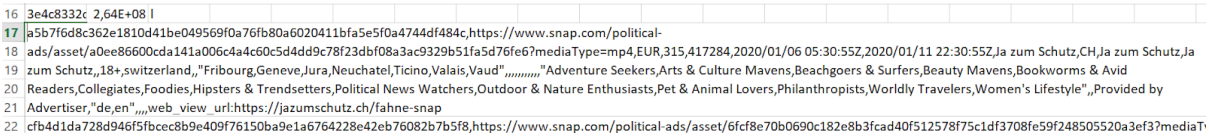
بعد از اینکه صفحه را بازآوری (Refresh) کنید اطلاعات تبلیغات بلینگ‌کت را خواهید دید. اگر آن حساب در ۷ روز گذشته هیچ تبلیغی را اجرا نکرده باشد، پیام «This account hasn't promoted any ads in the last seven days» را مشاهده خواهید کرد. از آنجایی که فقط می‌توانید تبلیغات ۷ روز گذشته را ببینید، بهترین کاری که می‌توانید انجام دهید این است که جستجوی خود را مرتبا تکرار کنید تا ببینید آیا یک حساب کاربری تبلیغاتی داشته یا خیر، و هر بار که آگهی‌های جدیدی می‌بینید از صفحه‌نمایش اسکرین‌شات بگیرید.

اسنپ چت

«کتابخانه‌ی تبلیغات سیاسی اسنپ» اطلاعاتی درباره‌ی تبلیغات سیاسی، تبلیغات «مرتبط با مسائل اجتماعی» و تبلیغات حمایتی ارائه می‌دهد. مورد آخر را «تبلیغات مربوط به موضوعات یا سازمان‌هایی که در سطح محلی، ملی یا جهانی موضوع بحث و یا دارای اهمیت عمومی هستند» تعریف کرده‌اند؛ به‌عنوان مثال، موضوعاتی مانند مهاجرت، آموزش عمومی یا اسلحه.

زمانی که به کتابخانه می‌روید فهرستی از سال‌های مختلف را مشاهده خواهید کرد:

با کلیک کردن روی هر کدام از سال‌ها می‌توانید صفحه‌ی گسترده‌ای شامل اطلاعات تمام تبلیغات آن سال را دانلود کنید. محتوای صفحه‌گسترده در نگاه اول خیلی هیجان‌انگیز به نظر نمی‌رسد، اما در واقع بسیار جالب است! هر خط نشان‌دهنده‌ی یک تبلیغ است و به شما نشان می‌دهد که چه کسی تبلیغ را منتشر کرده، چه مقدار برای آن هزینه شده، و حتی چه ویژگی‌های خاصی برای کاربران هدف انتخاب شده است.



در مثال بالا، تبلیغ‌کننده می‌خواست «ماجراجوها، دوستداران هنر و فرهنگ، ساحل‌بروها و موج‌سواران، علاقمندان به محصولات زیبایی، کتاب‌خوان‌ها و خوانندگان مشتاق، دانشگاهیان، متخصصان غذا، هیپسترها و پیشگامان مد، تماشاگران اخبار سیاسی، علاقه‌مندان به فضای باز و طبیعت، دوستداران حیوانات، نیکوکاران، کسانی که به دور دنیا سفر می‌کنند و علاقمندان به سبک زندگی زنان» را هدف قرار دهد.

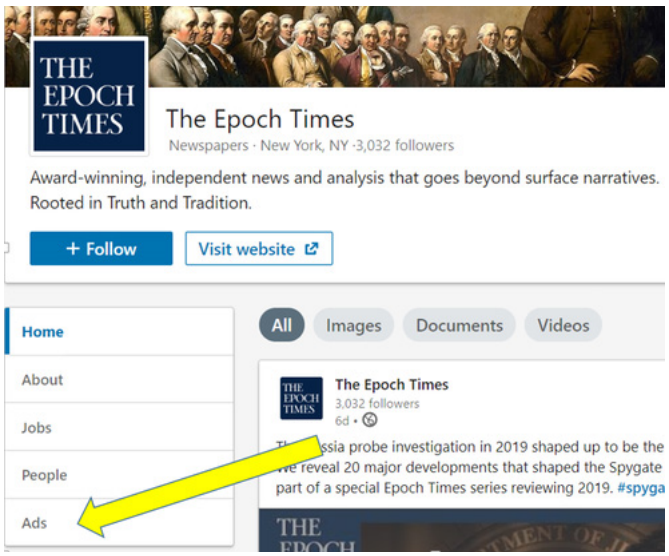
پلتفرم‌های دیگر این نوع اطلاعات را در کتابخانه‌های تبلیغات خود ارائه نمی‌کنند.

همچنین، در این صفحه‌ی گسترده یک URL نیز وجود دارد که به شما امکان می‌دهد خود آگهی منتشرشده را ببینید. در این مثال، من پیامی پیدا کردم که مردم را به خرید پرچم چندرنگ دگرباشان جنسی برای حمایت از رأی‌گیری آتی در سوئیس مربوط به محافظت در برابر تبعیض علیه افراد دگرباش جنسی تشویق می‌کرد.

لینکدین

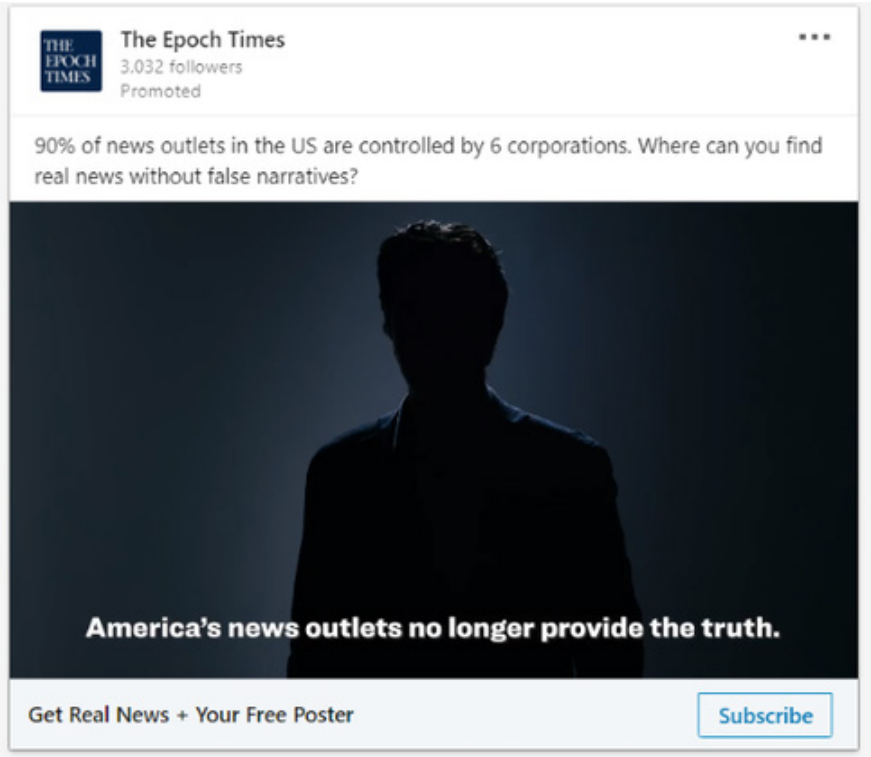
تبلیغات سیاسی در پلتفرم لینکدین ممنوع است و این پلتفرم کتابخانه‌ی تبلیغات نیز ندارد. خوشبختانه، راه دیگری برای بررسی تبلیغات یک شرکت خاص در پلتفرم وجود دارد.

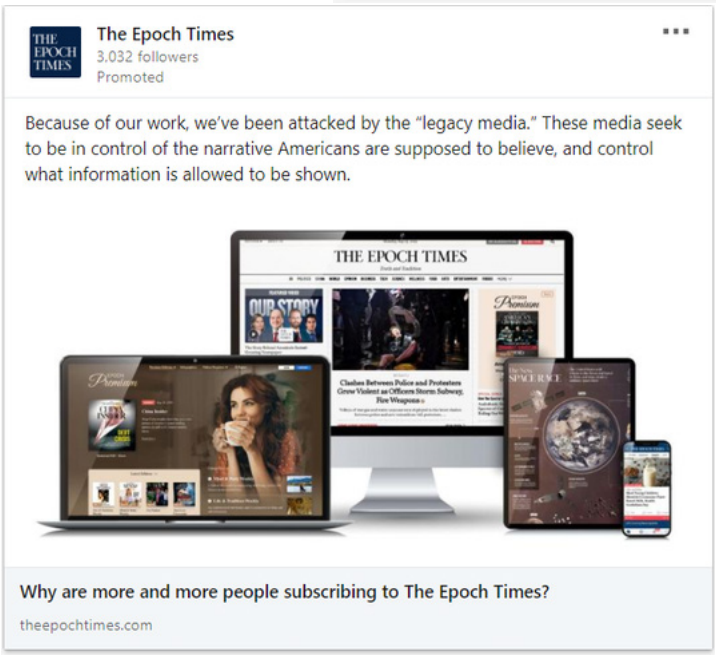
اگر به صفحه‌ی لینکدین شرکت مورد نظرتان بروید، گزینه‌ای به نام «Ads» را در پایین ستون سمت چپ مشاهده خواهید کرد.



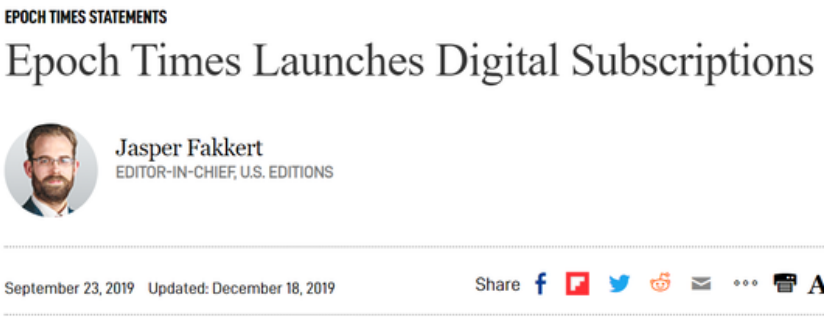
با کلیک کردن روی این گزینه فهرستی از تمام تبلیغات منتشرشده توسط آن شرکت در ۶ ماه گذشته را خواهید دید. با استفاده از این ویژگی، می‌توان مشاهده کرد که اپیاک تایمز پس از اینکه از انجام تبلیغات در فیس‌بوک منع شد، همچنان در حال انتشار تبلیغات در لینکدین بود.

دو آگهی این شرکت ادعا می‌کردند که «خبرگزاری‌های آمریکا دیگر حقایق را در اختیار شما قرار نمی‌دهند» و درمقابل، ایپاک تایمز را رسانه‌ای «مستقل» و «غیرحزبی» معرفی می‌کردند.





تاریخ دقیق انتشار تبلیغات قابل مشاهده نیست، اما می‌توانید روی تبلیغ کلیک کنید (حتی اگر تبلیغ مورد نظر در لینکدین فعال نباشد باز هم این کار ممکن است) و گاهی اوقات سایت مقصد تاریخ دقیق‌تری را در اختیارتان قرار خواهد داد. اولین آگهی ایپاک تایمز به متنی می‌رسید که در تاریخ ۲۳ سپتامبر ۲۰۱۹ منتشر و در تاریخ ۱۸ دسامبر ۲۰۱۹ به‌روزرسانی شده بود و می‌توانست به تخمین زدن زمان پخش آگهی کمک کند.


EPOCH TIMES STATEMENTS

Epoch Times Launches Digital Subscriptions

Jasper Fakkert
EDITOR-IN-CHIEF, U.S. EDITIONS

September 23, 2019 Updated: December 18, 2019

Share

اگر با امکانات و ویژگی‌های پنهان کتابخانه‌های تبلیغات آشنا شوید، تبدیل به گزینه‌ای آسان و قدرتمند در زرادخانه‌ی تحقیقات دیجیتال شما و عنصر مهمی برای انجام تحقیقات درباره‌ی یک شخص یا نهاد حاضر در رسانه‌های اجتماعی خواهند شد.

۱۰. دنبال کردن عاملان در فضای مجازی

نوشته‌ی: بن کالینز

بن کالینز خبرنگار ان‌بی‌سی نیوز است و تمرکز او بر اخبار نادرست، افراط گرایی و اینترنت است. در ۵ سال گذشته، او در مورد افزایش تئوری‌های توطئه، گروه‌های نفرت، کمپین‌های دستکاری خارجی و شکست پلتفرم‌ها گزارش داده است. او پیش از این در دیلی بیست مشغول فعالیت بود، جایی که به همراه تیمش حساب‌ها، گروه‌ها و رویدادهای واقعی ایجاد شده توسط مزرعه‌ی ترول‌های آژانس تحقیقات اینترنتی روسیه در طول انتخابات ۲۰۱۶ آمریکا را کشف کردند.

در ۳ آگوست ۲۰۱۹، پاتریک کروسیوس وارد یک فروشگاه والمارت در ال‌پاسو شد و با انگیزه‌ی ملی‌گرایی سفیدپوستی ۲۲ نفر را به ضرب گلوله کشت. اما قبل از اینکه وارد فروشگاه شود، مانیفستی را به گروه گفتگوی سیاسی در chan.net8 ارسال کرد: یک تالار گفتگو با قابلیت ناشناس ماندن که در سال‌های اخیر به محل تجمع ملی‌گرایان سفیدپوست تبدیل شده است. تالارهای گفتگوی سیاسی در ۴چن و ۸چن تقریباً به‌طور کامل بدون فیلتر هستند و محتواهای پست‌شده فیلتر و یا حذف نمی‌شوند و تا تابستان ۲۰۱۹، ۸چن به محل تجمع مطالب و بحث‌های خشونت‌آمیز ناسیونالیسم سفیدپوستی تبدیل شده بود.

می‌شود گفت تا حدی به همین دلیل بود که کاربران ۸چن گاهی اوقات که یک مانیفست جدید و خشونت‌آمیز در تالار گفتگو پست می‌شد به مقامات و روزنامه‌نگاران هشدار می‌دادند. این کار از طریق افزودن نظرات در زیر خود مانیفست و همچنین از طریق خبررسانی آنلاین به رسانه‌ها یا مجریان قانون انجام می‌شد. هنگامی که تیرانداز ال‌پاسو اولین بار مانیفست خود را ارسال کرد - که ابتدا با فایل پیوست اشتباهی پست شده بود - یکی از کاربران پاسخ داد «سلام، اف‌بی‌آی!». سپس مانیفست صحیح مستقیما در زیر نظری که از اف‌بی‌آی در آن نام برده شده بود ارسال شد.

این نوع خودگزارش‌دهی در پی فجایع می‌تواند اطلاعاتی حیاتی در اختیار روزنامه‌نگاران قرار دهد. در برخی موارد، کاربران خیرخواه‌تر مانیفست‌ها یا پست‌های مشکوکی را که قبل از تیراندازی ارسال شده

در فضاهای بازتر و اصلی‌تر مانند توئیتر و ردیت منتشر می‌کنند. این کار ضروری است چراکه به‌راحتی می‌توان متوجه یک پست یا اظهار نظر مرتبط در 4Chan و 8Chan نشد و آن را از دست داد.

پلتفرم‌های ناشناس مانند 4Chan و 8Chan نقش مهمی در اکوسیستم اطلاعات نادرست و دروغ‌پراکنی آنلاین و اوباشگری اینترنتی بازی می‌کنند، زیرا اغلب در این فضاها است که افراد با هم برای راه‌اندازی و هماهنگی کمپین‌ها همکاری می‌کنند. ردیت، یکی دیگر از فضاهای محبوب که در آن کاربران تا حد زیادی ناشناس هستند، میزبان مجموعه‌های متنوعی از جوامع آنلاین است. برخی از آن‌ها زیرمجموعه‌هایی هستند که کاربران می‌توانند در آن داستان‌های مربوط به سرگرمی‌ها یا نظرات خود درباره‌ی اخبار و رویدادها را تبادل کنند و محتوایشان به‌شدت تعدیل و فیلتر می‌شود. مجموعه‌های دیگری نیز هستند که اساسا ورود هر فرد یا محتوایی در آن‌ها آزاد است و نفرت می‌تواند در آن‌ها بی هیچ مانعی رشد کند. روزنامه‌نگاران باید بدانند چگونه همه‌ی این جوامع را نظارت کرده و از آن‌ها گزارش تهیه کنند و از پیچیدگی‌های نحوه‌ی عملکرد آن‌ها مطلع باشند.

با در نظر داشتن این موضوع، در اینجا چند قانون برای استفاده از 4Chan و 8Chan و جدیدترین نسخه‌ی این پلتفرم 8kun ذکر خواهیم کرد که زمانی که تحقیقات شما مستلزم استفاده از این فضاها برای یافتن اطلاعات بیشتر است، بهتر است آن‌ها را رعایت کنید:

۱. به هیچ چیز در 4Chan/8Chan اعتماد نکنید.

۲. به هیچ چیز در 4Chan/8Chan اعتماد نکنید.

۳. به هیچ چیز در 4Chan/8Chan اعتماد نکنید.

۴. بعضا ممکن است برخی اطلاعات مفید مربوط به (یا حتی شواهدی از) یک جنایت، کمپین ترولینگ یا اطلاعات نادرست در 4Chan/8Chan یافت شود.

۵. به هیچ چیز در 4Chan/8Chan اعتماد نکنید.

نمی‌توانم به اندازه‌ی کافی تأکید کنم که رعایت قوانین ۱، ۲، ۳ و ۵ برای خبرنگاران چقدر مهم است، حتی اگر آن‌ها را از دریافت مقداری از اطلاعات هیجان‌انگیز و مهمی که می‌توان از شماره‌ی ۴ به

دست آورد، محروم کند. این وب‌سایت‌ها به معنای واقعی کلمه برای اوباشگری، پخش محتوای کنایه‌آمیز و دروغ‌پردازی در مورد کسانی که دشمن فرض می‌شوند، انتشار دروغ‌هایی در مورد افراد به‌حاشیه‌رانده‌شده، و گاهی اوقات نیز پست کردن دروغ‌های بگویی‌نگویی خنده‌دار به‌عنوان داستان‌های واقعی در مورد دوران نوجوانی ساخته شده‌اند.

گواه این واقعیت نیز این است که این فضاها به‌عنوان محل تخلیه‌ی مانیفست‌های ملی‌گرایان سفیدپوست، اینسل‌ها (عزب‌های ناخواسته) و سایر تیراندازان مرد جوان دچار آسیب مورد استفاده قرار گرفته‌اند.

اجازه بدهید یک بار دیگر تکرار کنیم: اگر مطلبی روی 4Chan یا 8Chan باشد (که از اینجا به بعد علی‌رغم تغییر عنوان رسمی آن به 8kun به‌عنوان 8Chan به آن اشاره خواهیم کرد) به احتمال بسیار زیاد دروغی است که بنا است از طریق خبرنگاران بذر هرج‌ومرج و آشفتگی را بپاشد. هیچ مطلبی را پست نکنید، چون ممکن است هدف افرادی قرار بگیرید که وقت زیادی برای هدر دادن دارند!

تأیید مانیفست

دلیل اهمیت تلاش اعضای جوامعی مانند 8Chan برای جلب توجه به مانیفست‌ها یا سایر محتواهای خبرساز این است که این کار می‌تواند بسیار مفید باشد. اظهارنظر کاربری که زیر پست مانیفست تیرانداز ال‌پاسو نوشته بود «سلام، اف‌بی‌آی!» سرنخی بود که کمک کرد من از وجود مانیفست مطلع شوم. مدت کوتاهی پس از گزارش تیراندازی، توئیتر را با کلمات کلیدی‌ای مانند «El paso 4chan» و «El paso 8chan» جستجو کردم. جستجوی [city name] + [8chan or 4chan or incels.co] و یا سایر سایت‌های افراطی می‌تواند الگوی مفیدی برای هر رویداد مشابه باشد.

جستجوی من در توئیتر نشان داد که معدودی از کاربران اسکرین‌شات‌هایی از پست‌های ۸چن تیرانداز را به اشتراک گذاشته بودند، اگرچه بیشتر آن‌ها به اشتباه این پست را به شخصی در ۴چن نسبت داده بودند. بنابراین کاری که باید می‌کردم این بود که دنبال پست بگردم.

سریعترین راه برای جستجوی یک پست 8Chan چیست؟ گوگل. عبارت جستجوی من پس از واقعه‌ی تیراندازی "site:8ch.net" بود که بخشی از پست ادعایی 8Chan را هم به آن اضافه

کرده بودم (توجه داشته باشید که 4Chan پس از مدت زمانی مشخص پست‌ها را به‌طور خودکار از سرورهای خود حذف می‌کند، اما سایت‌هایی برای بایگانی محتوای 4Chan به‌صورت خودکار وجود دارند. جامع‌ترین آنها plebs.org4 است. پست‌های بایگانی‌شده‌ی 4Chan را می‌توان به‌سادگی با جایگزینی 4Chan در URL با plebs4 و حذف پیشوند "boards" پیدا کرد. به‌عنوان مثال:

boards.4chan.org/pol/13561062.html could be found at 4plebs.org/pol/13561062.html.)

در برخی تیراندازی‌ها جستجوی "'site:4chan.net + 'manifesto' or 'fbi"' و استفاده از گزینه‌های جستجوی گوگل برای محدود کردن محدوده‌ی زمانی جستجو به ۲۴ ساعت گذشته ممکن است مفید باشد. ممکن است کاربران تلاش کرده باشند با پاسخ‌ها و اظهارنظرهای خود قصد ارسال‌کننده‌ی پست را برملا و توجه‌ها را به آن جلب کنند.

استراتژی اولیه‌ی من برای جستجو، پست 8Chan مورد نظر را نشان نداد و همین باعث شد فکر کنم پست درواقع مطلب جعلی‌ای بوده که پس از تیراندازی به‌سرعت ایجاد شده است. اما به نظر می‌رسید چیزی در این میان سر جای خودش نیست. پستی که در اسکرین‌شات‌های توئیتر دیده می‌شد دارای شناسه‌ی کاربر و شماره‌ی پست بود. همین باعث شد باور کنم که با یک پست واقعی سروکار دارم، نه یک جعل ساده. در 8Chan هر پست از یک شناسه‌ی کاربری منحصربه‌فرد می‌آید که به‌صورت الگوریتمی تولید و در کنار تاریخ پست نمایش داده می‌شود. این سیستم به کاربران این امکان را می‌دهد که یک شناسه‌ی ثابت داشته باشند و بتوانند خود را در یک رشته پست شناسایی کنند.

جالب است بدانید که این سیستم برای ایجاد شناسه‌های کاربری همان سیستمی است که باعث می‌شود افراد بتوانند کاربر Q مرتبط با تئوری توطئه‌ی QAnon را شناسایی کنند. هنگام ارسال یک پست، کاربرها می‌توانند با وارد کردن یک نام کاربری در بخش مربوط به شناسه‌ی کاربر و به دنبال آن یک # و پس از آن یک رمز عبور، نام کاربری و رمز عبور دائمی ایجاد کنند.

با استفاده از شناسه‌ی کاربری من متوجه شدم شخصی که به اشتباه فایل پی‌دی‌افی را که نام تیرانداز بر آن بوده ارسال کرده، همان کاربری است که مانیفست واقعی را دو دقیقه‌ی بعد ارسال کرده است. هر دو پست شناسه‌ی کاربری تصادفی یکسانی داشتند: b58820.

در کنار شناسه‌ی کاربری یک شماره پست وجود دارد که تا حدودی دائمی است و یک URL منحصربه‌فرد برای هر پست ایجاد می‌کند. اسکرین‌شات مانیفست ال‌پاسو که در توئیتر به اشتراک گذاشته شده بود، شماره پست "No.13561062" را نشان می‌داد. URL مرتبط با این شماره پست به این شکل خواهد بود: "8ch.net/pol/res/13561062.html". می‌توانید از این الگوی URL در هر دوی 4Chan و 8Chan استفاده کنید.

اما در این مورد، پستی وجود نداشت. فکر کردم شاید پست حذف شده باشد (بعدتر متوجه شدم که جیم واتکینز، مالک 8Chan، پس از اطلاع از محتوای پست، آن را حذف کرده است).

با از بین رفتن پست، آخرین امید من این بود که شاید کسی که اهمیت آن را تشخیص داده بایگانی‌اش کرده باشد. خوشبختانه، یک کاربر خوش‌فکر 8Chan پست را در سایت آرشیو archive.is ذخیره کرده بود. با وارد کردن URL در کادر "I want to search the archive for saved snapshots" در سایت archive.is مشخص شد که پست مانیفست واقعی بود و می‌توانستم آن را مشاهده کنم.

اما مشکل دیگری هم وجود داشت: پست اولین بار چه زمانی در 8Chan ارسال شده بود؟ من به یک برچسب زمان دقیق نیاز داشتم تا مطمئن شوم که مانیفست قبل از شروع حمله تیرانداز ال‌پاسو پست شده است.

4Chan و 8Chan هر دو برچسب‌های زمانی خود را محلی‌سازی می‌کنند و این استخراج زمان واقعی از سایت‌های بایگانی را به یک کار پیچیده تبدیل می‌کند. خوشبختانه راه‌حل قابل اطمینانی برای حل این مشکل وجود دارد. بر روی برچسب زمان کلیک‌راست کنید و سپس گزینه‌ی "inspect element" را انتخاب کنید. این کار کد منبع سایت را به شما نشان خواهد داد و بخشی را که با عبارت "<number] =unixtime time[شروع می‌شود برایتان برجسته خواهد کرد. عددی را که مشاهده می‌کنید در یک تبدیلگر زمان یونیکس، مثل unixtimestamp.com، وارد کنید و زمان ارسال پست را تا ثانیه‌ی دقیق آن بر حسب ساعت هماهنگ جهانی (یوتی‌سی) دریافت خواهید کرد. تبدیل زمان از یوتی‌سی به زمان محلی ال‌پاسو نشان داد که مانیفست در ساعت ۱۰:۱۵ صبح به وقت منطقه‌ی زمانی مرکزی پست شده است - دقایقی قبل از شروع تیراندازی.

این کار به من کمک کرد بفهمم که مانیفست ارسال‌شده در 8Chan درواقع مدرک مشروع و محکمه‌پسندی از یک اقدام تروریستی نژادپرستانه‌ی داخلی است.

ردیابی عاملان در پلتفرم‌های مختلف

در سال ۲۰۱۷، لین دیویس، یک «محقق گیمرگیت» (بخوانید: تعقیب‌کننده‌ی اینترنتی حرفه‌ای) که برای مایلو یناپولُس، شخصیت رسوای راست افراطی آلترناتیو کار می‌کرد، پدرش را در خانه‌اش کشت. دیویس با والدینش وارد مشاجره شده بود و تماسی که با پلیس ۹۱۱ گرفته شده بود نشان می‌داد که مدت کوتاهی قبل از حمله، در حال فریاد زدن مشتی اصطلاحات راست افراطی اینترنتی بوده است. او قبل از اینکه پدرش با پلیس تماس بگیرد و از آن‌ها برای بیرون انداختن پسرش که هنوز با آن‌ها زندگی می‌کرد کمک بخواهد، والدینش را چپ‌های پدوفیل خطاب کرده بود.

دیویس در فضای آنلاین با نام“Seattle4Truth” شناخته می‌شد و در ویدئوهای یوتیوبش اغلب به حلقه‌های پنهانی پدوفیلی که معتقد بود نیروی محرکه‌ی لیبرالیسم هستند اشاره می‌کرد. یکی از ویدئوهای یوتیوب او با عنوان «پیوندهای عمیق ایدئولوژی مترقی با پدوفیلی» بسیار شناخته شده بود.

یکی از سناریوهای رؤیایی خبرنگاران در تحقیقات افراط‌گرایی در فضای آنلاین مجرمی است که از یک نام کاربری ثابت در تمام پلتفرم‌ها استفاده کند و دیویس دقیقا چنین موردی بود. او در یوتیوب و در ردیت جایی که محتوای پست‌هایش حتی بیشتر از یوتیوب نشان از یک مغز توطئه‌زده داشت- از نام کاربری ”Seattle4Truth“ استفاده می‌کرد.

این نکته چگونه کشف شد؟ با قرار دادن نام کاربری ”Seattle4truth“ در الگوی URL ردیت:

reddit.com/u/[username] بعد از پیدا کردن کاربر مورد نظر، می‌توانید محتوای پست‌شده توسط او را بر اساس جدیدترین پست‌ها، محبوب‌ترین پست‌ها و «جنجال‌برانگیزترین» پست‌ها -که بر اساس ترکیبی از تعداد دفعاتی که رأی مثبت و منفی دریافت کرده‌اند رتبه‌بندی می‌شوند- مرتب‌سازی کنید.

یکی از راه‌های بررسی سریع نام‌های کاربری استفاده از Namechk است که یک نام کاربری را در نزدیک به صد سرویس اینترنتی جستجو می‌کند. همانطور که در زیر نیز توضیح خواهم داد، این بدان معنی نیست که شخص یکسانی همه‌ی این حساب‌ها را اداره می‌کند، اما با استفاده از این روش می‌توانید بفهمید در چه پلتفرم‌هایی از نام کاربری مورد نظر استفاده شده است و سپس شروع به تحقیقات بیشتر کنید. همچنین می‌توانید نام کاربری مورد نظرتان را در گوگل نیز جستجو کنید.

به‌علاوه، باید به جوامع اینترنتی بسیار خاصی که کاربر مورد نظرتان ممکن است در آن‌ها فعال باشد نیز توجه کنید. تیرانداز مدرسه‌ای در نیومکزیکو در سال ۲۰۱۷، به نام ویلیام ادوارد آچیسون، توسط کاربران در KiwiFarms، سایتی که عمدتاًبه قلدری ضد تراجنسیتی اختصاص دارد، با نام کاربری @satanicdruggie شناسایی شد.

آچیسون نه تنها در دانشنامه‌ی دراماتیکا فعال بود، بلکه یک اپراتور سیستم (SysOp) نیز محسوب می‌شد و از کاربران پیشرفته و خبره بود (ما از طریق کاربرانی در سایت که با آچیسون روابطی عمدتا از طریق اسکایپ ایجاد کرده بودند مطمئن شدیم که حساب‌ها متعلق به او هستند. در صورتی که یکی از حساب‌های کاربری آچیسون از فعالیت منع می‌شد، او داوطلبانه نام‌های کاربری دیگرش را در اختیار افراد قرار می‌داد). جستجوی نام کاربری او در گوگل با استفاده از عبارت
"site:encyclopediadramatica.rs + [username]" نشان داد که او بیشتر با نام کاربری "Satanic Druggie" شناخته می‌شده اما از نام‌های دیگری مانند "Future School Shooter" و "Adam Lanza" (نام تیرانداز سندی هوک) نیز استفاده می‌کرده است.
تاریخچه‌ی پست‌های او در سراسر وب نشان‌دهنده‌ی نوعی وسواس فکری درباره‌ی تیراندازی در مدرسه بود که حتی پس از تیراندازی پلیس موفق به کشف آن نشده بود.

باز هم لازم است تأکید کنیم که وجود یک نام کاربری در پلتفرم‌های مختلف تضمینی بر اینکه تمام آن حساب‌ها متعلق به یک شخص باشد نیست.

در یک مثال معروف، ایان مایلز چئونگ، مایک سرنوویچ، اینفو وارز و گِیت‌وِی پاندیت، عوامل بدنام راست افراطی، همگی ادعا کردند مردی که در رقابت‌های قهرمانی بازی‌های ویدئویی جکسون‌ویل دو نفر را کشته و ۱۰ نفر را مجروح کرده بود، ضد ترامپ است.

دلیلشان چه بود؟ تیرانداز، دیوید کتز، در رقابت‌های قهرمانی بازی‌های کامپیوتری از نام کاربری "Ravens2012Champs" استفاده می‌کرد و یک کاربر ضدترامپ در ردیت نیز نام کاربری مشابهی داشت: "RavenChamps".

پوشش خبری این ادعا به همان اندازه که اشتباه بود جالب و گیرا هم بود. در سرتیتر اینفو وارز آمده بود: « تیرانداز جکسونویل در ردیت از "ترامپتاردها" (طرفداران ترامپ) انتقاد کرده بود» و داستان ادعا می‌کرد که تیرانداز «از حامیان ترامپ متنفر است».

درنهایت کاشف به عمل آمد که نام کاربری "RavenChamps" متعلق به فردی کاملا متفاوت است؛ مردی به نام پاول اهل مینه‌سوتا که به کارگری در یک کارخانه اشتغال داشت.

چند ساعت پس از تیراندازی، پاول در توئیتر نوشته بود: «من زنده‌ام، می‌دونید که؟!» (تیراندز اصلی پس از حمله به زندگی خود پایان داده بود).

شما قطعا به اطلاعاتی بیش از یک نام کاربری نیاز دارید، اما نام کاربری می‌تواند نقطه‌ای کلیدی برای شروع و تماس با مجری قانون، بررسی سوابق عمومی و برقراری تماس‌های تلفنی باشد.

ردیابی کمپین‌ها هم‌زمان با وقوع

کمپین‌های اطلاعات نادرست و دستکاری رسانه‌ای اغلب در ردیت و ۴چن پخش می‌شوند و برخی از آن‌ها را می‌توان هم‌زمان با وقوع ردیابی کرد.

به عنوان مثال، 4Chan سال‌هاست که به تقلب در نظرسنجی‌های آنلاین برای تقویت نامزدهای خاص پرداخته است. در سال ۲۰۱۶، به‌هنگام نظرسنجی‌هایی که پس از مناظره‌ها انجام می‌شد اعضای 4Chan مکررا لینک‌هایی را که نامزد مرجح کاربران، ترامپ، را تبلیغ می‌کردند به سایت‌های خبری ملی و محلی ارسال می‌کردند.

تغییر پارامترهای جستجوی گوگل و انتخاب گزینه‌ی "last hour" برای غربال نتایج و سپس جستجوی "site:4chan.org 'polls'" ایده‌ی خوبی از نظرسنجی‌هایی که کاربران ۴چن سعی در دستکاری آن‌ها در زمان واقعی دارند به شما می‌دهد.

همین روند در دور بعدی انتخابات نیز ادامه داشت. این بار 4Chan در نظرسنجی‌ها به تولسی گبرد کمک می‌کرد؛ نامزدی که در دراج پیورت و NJ.com. به او لقب "Mommy" داده بودند. با یک جستجوی ساده در گوگل، هر کسی می‌توانست ببیند که نتایج نظرسنجی‌ها در زمان واقعی و پس از اینکه یکی از کاربران 4Chan به باقی کاربران گفت «با تمام قدرت حمایتش کنید» تغییر داده شده است.

دنبال کردن فعالیت‌های ترولینگ به‌صورت هم‌زمان در سایت‌هایی مانند انجمن "r/The_Donald"در ردیت به خاطر عملکرد "rising" خاص این پلتفرم، ساده‌تر نیز هست.

با استفاده از عبارت"reddit.com/r/[subreddit-name]/rising" پست‌هایی که در هر زمان در یک ساب‌ردیت با سرعتی غیرمعمول در حال جلب توجه و تعامل هستند مشخص می‌شوند.

همچنین می‌توانید پست‌هایی را که عملکردی بیشتر از پست‌های دیگر در سطح کل ردیت دارند نیز مشاهده کنید: reddit.com/r/all/rising. بیشتر پست‌ها از تمام انجمن‌های ردیت در اینجا ذخیره می‌شوند. البته این گزینه محتوای ساب‌ردیت‌های قرنطینه‌شده، که اغلب محتواهای بسیار نامناسبی منتشر می‌کنند و انجمن‌های دیگر را مورد حمله‌ی ترولینگ قرار می‌دهند، را ذخیره نمی‌کند. ساب‌ردیت‌های قرنطینه‌شده در گوگل هم موجود نیستند اما می‌توان با استفاده از عبارت جستجوی "reddit.com/r/[subreddit-name]/rising" آن‌ها را پیدا کرد. قرنطینه برای محدود کردن دسترسی کمپین‌های ترولینگ به خارج از حلقه‌ی مخاطبان متمرکزشان گزینه‌ی بسیار خوبی است، اما ردیابی نحوه‌ی سازماندهی عاملان بد در لحظه را دشوارتر می‌کند.

به‌طور کلی، ایده‌ی خوبی است که در جریان رویدادهای بزرگ سیاسی، تراژدی‌ها و انتخابات، آن بخشی از جوامع آنلاین را که مانند r/the_donald به خاطر کمپین‌های ترولینگ معروف هستند، زیر نظر داشته باشید.

واقعیت این است که گاهی اوقات کارهایی که این پلتفرم‌ها برای خنثی کردن تلاش‌های عاملان بد انجام می‌دهند می‌تواند انجام کارها را برای خبرنگاران دشوارتر کند. ابزارها می‌توانند کمک کنند، اما بسیاری از بررسی‌ها نیز باید به‌صورت دستی انجام شوند و انجامشان نیازمند روش‌های تأییدی است که الگوریتم‌ها و رایانه‌ها قادر به انجام آن نیستند.

دست‌آخر، یک کامپیوتر نمی‌تواند در این حوزه جایگزین انسان شود. خودمان باید دست‌به‌کار شویم.

۱۱. تجزیه و تحلیل شبکه و انتساب

نوشته‌ی: **بن نیمو**

بن نیمو مدیر تحقیقات در گرافیکا و کارشناس ارشد غیردائم در آزمایشگاه تحقیقات قانونی دیجیتال شورای آتلانتیک است. او در مطالعه‌ی اطلاعات در مقیاس بزرگ و در پلتفرم‌های مختلف و همچنین در زمینه‌ی عملیات تأثیرگذاری تخصص دارد. بن اوقات فراغتش را زیر آب می‌گذراند، جایی که نمی‌توان با تلفن همراهش تماس گرفت.

هنگام برخورد با هر عملیات اطلاعاتی مشکوک، یکی از سؤالات کلیدی برای هر محقق این است که ابعاد عملیات چه اندازه است و تا کجا گسترش می‌یابد. این امری متفاوت از اندازه‌گیری تأثیر یک عملیات است که به‌نوبه‌ی خود اهمیت زیادی دارد. اینجا هدف پیدا کردن تمام حساب‌های کاربری و وب‌سایت‌هایی است که توسط عملیات اداره می‌شوند.

برای یک محقق، هدف این است که قبل از گزارش کردن عملیات تا جای ممکن آن را بررسی کند، زیرا زمانی که عملیات گزارش شد، می‌توان انتظار داشت که عاملان آن احتمالا با حذف یا رها کردن سایر دارایی‌ها- مخفی شوند.

اولین حلقه‌ی زنجیره

در هر تحقیقی پیدا کردن اولین سرنخ دشوارترین کار است. تحقیقات اغلب با راهنمایی یک کاربر نگران و یا (به‌ندرت) با اطلاع‌رسانی از طرف خود پلتفرم شبکه‌ی اجتماعی آغاز می‌شود. کار آزمایشگاه تحقیقات قانونی دیجیتال برای افشای عملیات اطلاعاتی روسیه با نام سِکِندِری اینفکشن با اطلاع‌رسانی فیس‌بوک آغاز شد که ۲۱ حساب مشکوک را در پلتفرم خود پیدا کرده بود. کار تحقیقات ۶ ماه بعد و زمانی به نتیجه رسید که گرافیکا، رویترز و ردیت عملیاتی را که هدف آن مداخله در انتخابات بریتانیا بود افشاء کردند. در مثالی دیگر، تحقیقات درباره‌ی یک کمپین اطلاعات نادرست که کهنه‌سربازان آمریکایی را هدف قرار می‌داد با اطلاع‌رسانی از طرف یکی از کارمندان سازمان غیرانتفاعی

کهنه‌سربازان جنگ ویتنام آغاز شد که متوجه شده بود گروهی با نام این سازمان در فیس‌بوک فعالیت می‌کند و دوبرابر دنبال‌کننده‌های صفحه‌ی واقعی سازمان نیز دنبال‌کننده دارد.

هیچ قانون واحدی برای شناسایی اولین حلقه‌ی زنجیره از طریق منابع شخصی شما وجود ندارد. مؤثرترین استراتژی گشتن به دنبال موارد نامتجانس است. این عدم تجانس می‌تواند حساب کاربری‌ای باشد که کاربر آن ظاهرا در تنسی مستقر است اما با شماره‌ی تلفن همراهی از روسیه ثبت شده است. و یا می‌تواند صفحه‌ی فیس‌بوکی باشد که ادعا می‌کند از نیجر اداره می‌شود اما در واقع از سنگال و پرتغال اداره می‌شود. و یا می‌تواند یک حساب یوتیوب با میلیون‌ها بازدید باشد که در سال ۲۰۱۹ حجم زیادی محتوا در حمایت از چین پست کرده، اما تقریبا تمام بازدیدهای آن مربوط به قسمت‌هایی از کمدی‌های بریتانیایی است که در سال ۲۰۱۶ بارگذاری کرده است.

به‌همین‌ترتیب، سرنخ اولیه‌ی شما می‌تواند وب‌سایت ناشناسی باشد که تمرکزش بر موضوعات سیاست خارجی آمریکا است اما توسط خزانه‌داری منطقه‌ی نظامی خاور دور فدراسیون روسیه ثبت شده است. و یا می‌تواند مصاحبه‌ای با یک مأمور ام‌آی۶ باشد که در قالب زبان انگلیسی فاخر و به سبک شکسپیر پنهان شده است و یا حساب توییتری که دعوتنامه‌هایی به سایت‌های پورنوگرافی را در بین نقل‌قول‌هایی از رمان عقل و احساس جین آستن پنهان کرده و پخش می‌کند.

ترفند مهمی که می‌توانید برای تمام این سرنخ‌ها به کار ببندید این است که زمان کافی به آن‌ها اختصاص بدهید و خوب درباره‌شان فکر کنید. چه بسا زمان‌هایی که روزنامه‌نگاران و محققان به دلیل ضیق وقت با اظهارنظر ساده‌ای مثل «چه عجیب!» از کنار چنین سرنخ‌هایی می‌گذرند. نکته‌ی مهم این است که چیزهای عجیب اغلب بی‌دلیل عجیب نیستند. زمانی که به چیز عجیبی برمی‌خورید، می‌توانید وقت بگذارید و از خودتان بپرسید: چرا اینطور است؟ این می‌تواند قدم اول شما در افشای یک عملیات جدید باشد.

داشته‌ها، رفتار، محتوا

هنگامی که داشته اولیه - مانند یک حساب کاربری یا یک وب‌سایت - شناسایی شد، چالش بعدی این است که مشخص کنیم این داشته به کجا منتهی می‌شود. در اینجا سه سؤال حیاتی برگرفته از الفبای دروغ‌پراکنی نوشته‌ی کامیل فرانسوا را می‌توان مطرح کرد:

- **چه اطلاعاتی در مورد این دارایی اولیه در دسترس داریم؟**
- **عملکرد و رفتار این دارایی چگونه بوده است؟**
- **چه محتوایی را پست کرده است؟**

اولین مرحله این است که تا حد امکان اطلاعات بیشتری در مورد داشته اولیه جمع‌آوری کنید. اگر با یک وب‌سایت سروکار دارید، چه زمانی و توسط چه کسی ثبت شده است؟ آیا مشخصه‌ی قابل شناسایی‌ای مانند کد گوگل آنالتیکس یا شناسه‌ی گوگل ادسنس، آدرس ایمیل ثبت‌نام یا شماره تلفن دارد؟ چنین سؤالاتی را می‌توان با استفاده از سوابق تاریخی Whols، ارائه شده توسط سرویس‌هایی مانند domainbigdata.com، domaintools.com، lookup.icann.com یا spyonweb.com (که نامش تا حدودی دلهره‌آور است) بررسی کرد.


Domain Information

Name: nbenegroup.com

Registry Domain ID: 1558058690_DOMAIN_COM-VRSN

Domain Status:
clientTransferProhibited

Nameservers:
dns1.netbreeze.net
dns2.netbreeze.net

Dates

Registry Expiration: 2020-06-04 06:17:42 UTC

Registrar Expiration: 2020-06-04 06:17:42 UTC

Created: 2009-06-04 06:17:42 UTC

Contact Information

Registrant:

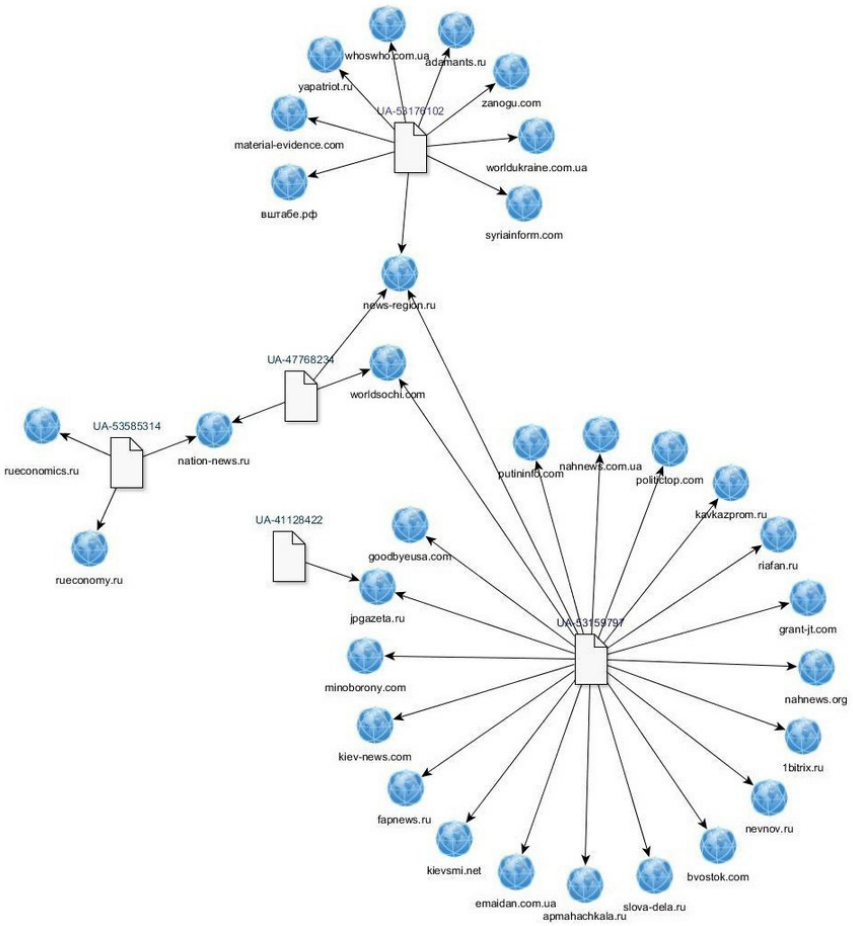
Name: Finance Department of the Far Eastern Military district

جزئیات ثبت وب‌سایت NBeneGroup.com، که ادعا می‌کرد یک «گروه تجزیه و تحلیل مختص جوانان» است اما ثبت آن به نام خزانه‌داری ناحیه‌ی نظامی خاور دور فدراسیون روسیه صورت گرفته بود که با استفاده از سوابق Whols در lookup.icann.org استخراج شده است.

از اطلاعات وب‌سایت می‌توان برای جستجوی داشته‌های دیگر استفاده کرد.
هم domaintools.com و هم spyonweb.com به کاربران این امکان را می‌دهند که با استفاده از شاخص‌هایی مانند آدرس IP و کد گوگل آنالتیکس وب‌سایت‌های وابسته‌ی احتمالی را جستجو کنند اگرچه عملیات‌های اطلاعاتی پیشرفته‌تر در حال حاضر اغلب اطلاعات ثبتی خود را در پشت نام

نهادهای تجاری یا خدمات حریم خصوصی پنهان می‌کنند و این تحقیقات را دشوارتر می‌کند.

لارنس الکساندر، محقق بریتانیایی، در یکی از تحلیل‌های اولیه‌ی خود موفق شد ۱۹ وب‌سایت را که توسط آژانس تحقیقات اینترنت روسیه اداره می‌شوند، با دنبال کردن کدهای گوگل آنالتیکس آن‌ها شناسایی کند. در آگوست ۲۰۱۸، شرکت امنیتی فایِر آی موفق شد یک عملیات تأثیرگذاری در مقیاس بزرگ که توسط ایران راه‌اندازی شده بود را از طریق اطلاعات ثبت وب‌سایت، از جمله ایمیل، شناسایی و روابط بین وب‌سایت‌هایی که در ظاهر ارتباطی با هم نداشتند را برملا کند.



شبکه‌ای از وب‌سایت‌های مرتبط با کدهای گوگل آنالتیکس یکسان (اعداد ۸ رقمی با پیشوند UA) که توسط محقق بریتانیایی لارنس الکساندر شناسایی شده است.

اگر داشته اولیه یک حساب کاربری در یک رسانه اجتماعی باشد، راهنمایی‌های ارائه‌شده در دو فصل قبل در مورد ربات‌ها و فعالیت‌های غیرواقعی و بررسی حساب‌های اجتماعی باید اعمال شوند. حساب کاربری چه زمانی ایجاد شده است؟ آیا نام کاربری‌ای که روی صفحه دیده می‌شود با نام صاحب حساب کاربری مطابقت دارد؟ (اگر شناسه‌ی صاحب حساب کاربری "@moniquegrieze" باشد و نام کاربری‌ای که روی صفحه مشاهده می‌کنید "Simmons Abigayle" باشد، این یعنی یا حساب هک و دزدیده شده و یا یکی از چندین حسابی است که به‌صورت هم‌زمان برای فعالیت‌های غیرواقعی ایجاد شده است).

سه حساب توئیتر که در یک عملیات بزرگ رباتی در آگوست ۲۰۱۷ شرکت داشتند. نام‌های روی صفحه را با نام کاربر مقایسه کنید. این عدم مطابقت نشان می‌دهد که به احتمال زیاد اینها حساب‌هایی هستند که توسط صاحب ربات‌ها ربوده، تغییر نام و تغییر کاربری داده شده‌اند.

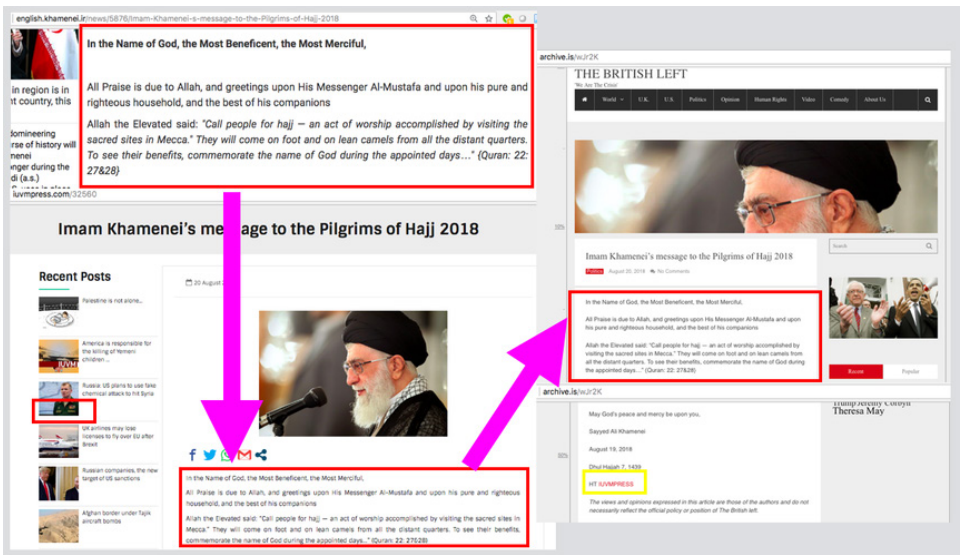
آیا حساب کاربری جزئیاتی قابل صحت‌سنجی در خصوص هویت کاربر و یا لینک‌هایی به دارایی‌های دیگر او در همان پلتفرم یا سایر پلتفرم‌ها ارائه می‌دهد؟ اگر با یک صفحه یا گروه فیس‌بوک سروکار

دارید چه کسی و از کجا آن را مدیریت می‌کند؟ این کاربر چه کسانی را دنبال می‌کند و دنبال‌کنندگانش چه کسانی هستند؟ تنظیمات "Page transparency" و "group members" در فیس‌بوک و مشخصات پروفایل مانند زمان ایجاد حساب کاربری و تعداد کل توئیت‌ها و لایک‌ها در توئیتر اغلب می‌توانند سرنخ‌های ارزشمندی ارائه دهند. (در فیس‌بوک و اینستاگرام، دیدن تاریخ ایجاد حساب امکان‌پذیر نیست، اما تاریخ بارگذاری اولین عکس پروفایل اغلب می‌تواند جایگزین معقولی باشد.)

شفافیت اطلاعاتی وب‌سایت و صفحه‌ی فیس‌بوک سایتی به نام "C'est faux Les fake news du Mali" (نادرست است! اخبار جعلی از مالی) که در ظاهر کارش راستی‌آزمایی است و ادعا می‌کند توسط گروهی از دانشجوها در مالی اداره می‌شود، اما اداره‌ی سایت در واقع از سنگال و پرتغال صورت می‌گیرد. عکس از: DFRLab.

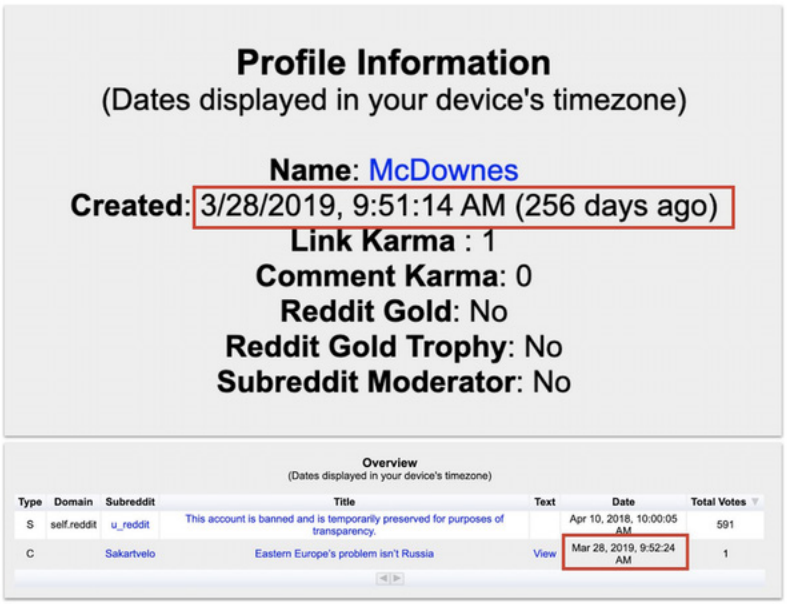
بعد از به دست آوردن تمام جزئیات ممکن در مورد داشته مورد نظر، نوبت به بررسی رفتار و فعالیت‌های آن می‌رسد. سؤال مهم در این مرحله این است: «ویژگی اصلی فعالیت‌های سوژه‌ی مورد نظر، که ممکن است به شناسایی سایر سوژه‌های درگیر در عملیات نیز کمک کند، چیست؟»

این سؤالی کلی است و می‌تواند پاسخ‌های متفاوت بسیاری داشته باشد؛ پاسخ‌هایی که بعضا ممکن است در مراحل پیشرفته‌تر تحقیقات به آن‌ها دست پیدا کنیم. به‌عنوان مثال برخی کانال‌های یوتیوب وجود دارند که علی‌رغم نام‌ها و عکس‌های پروفایل غربی عمدتا محتوای سیاسی به زبان چینی مخلوط با حجم زیادی از ویدئوهای کوتاه تیک‌تیک را ارسال می‌کنند. گاهی نیز ممکن است با مجموعه‌ای حساب‌های کاربری در فیس‌بوک یا توئیتر سروکار داشته باشیم که همیشه لینک‌هایی به یک وب‌سایت مشخص یا مجموعه‌ای از وب‌سایت‌های خاص ارسال می‌کنند. گاهی نیز با حساب‌های کاربری‌ای روبرو می‌شویم که از متن‌هایی یکسان یا با تفاوت‌های جزئی در بیوگرافی حساب خود استفاده می‌کنند. بعضی حساب‌های کاربری که در ظاهر متعلق به «خبرنگاران» هستند، هیچ مشخصه‌ی فردی قابل صحت‌سنجی‌ای ندارند و یا جزئیاتی ارائه می‌دهند که نادرستی آن قابل اثبات است. گاهی نیز عملیات شامل وب‌سایت‌هایی است که بیشتر محتوای خود را از سایت‌های دیگر سرقت می‌کنند، و فقط مقاله‌های گاه به گاه حزبی، جنجالی یا فریبنده تولید می‌کنند. ویژگی‌هایی از این دست بسیارند و چالش اصلی پیش روی محققان این است که با شناسایی مجموعه‌ای از این ویژگی‌ها بتوانند به نقطه‌ای برسند که بگویند: این داشته بخشی از این عملیات خاص است.



الگوی خاص فعالیت: مقاله‌ای که ابتدا در وب‌سایت آیت‌الله خامنه‌ای در ایران منتشر شده بود، متعاقبا بدون ذکر منبع توسط IUVMpress.com و britishleft.com، دو وب‌سایت در یک شبکه‌ی پروپاگاندای ایرانی، تکثیر شد. عکس از: DFRLab.

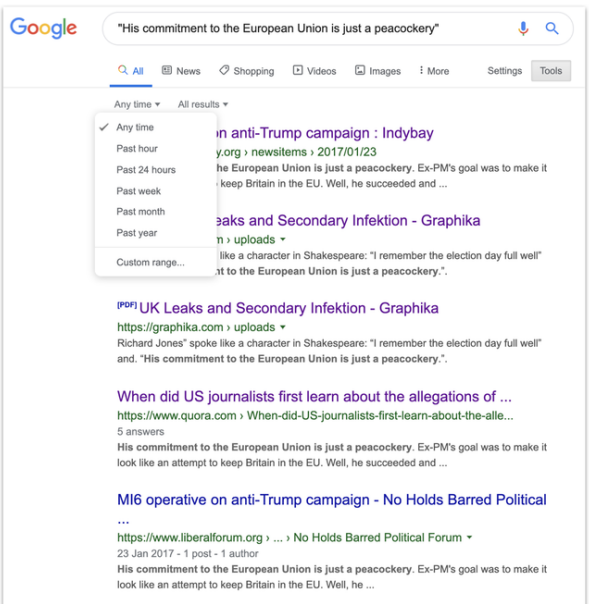
گاهی عدم وجود مشخصات فردی می‌تواند خود یک مشخصه باشد. در کمپین سِکِندِری اینفکشن «Secondary Infektion» از روسیه اوضاع از همین قرار بود. این کمپین از صدها حساب کاربری در پلتفرم های مختلف وبلاگ‌نویسی استفاده کرده بود که همه حاوی حداقل جزئیات مربوط به مشخصات فردی بودند، یک مقاله در روز ایجادشان پست کرده بودند و سپس رها شده و دیگر مورد استفاده قرار نگرفته بودند. این مشخصه به‌قدری در تمام حساب‌های متعلق به عملیات به یکسان تکرار شده بود که در طول تحقیقات به‌عنوان امضای عملیات شناخته شد. زمانی که حساب‌های ناشناس درست قبل از انتخابات عمومی بریتانیا در دسامبر ۲۰۱۹ شروع به انتشار اسناد تجاری لو رفته از ایالات متحده و بریتانیا کردند، گرافیکا و رویترز نشان دادند که این حساب‌ها دقیقا با این امضاء مطابقت دارند. ردیت نیز این تحلیل را تأیید کرد.



حساب کاربری به نام "McDownes," در ردیت که توسط پلتفرم ردیت با عملیات سکندری اینفکشن ارتباط داده شده است. حساب در تاریخ ۲۸ مارس ۲۰۱۹ ایجاد شده، چند دقیقه بعد از ایجاد یک مقاله پست کرده و پس از آن هیچ فعالیتی نداشته است. عکس از: گرافیکا. داده‌ها از: redective.com.

سرنخ‌هایی که از محتوا به دست می‌آورید می‌تواند به شناسایی سایت‌ها و اکانت‌هایی که بخشی از یک شبکه‌ی یکسان هستند نیز کمک کند. اگر سایت یا اکانت مورد نظر عکس یا میمی را به اشتراک گذاشته بهتر است آن را جستجوی معکوس کنید تا ببینید در چه جاهای دیگری از آن استفاده شده است. افزونه‌ی RevEye برای مرورگرهای وب ابزار بسیار مفیدی است که به محققان امکان می‌دهد جستجوی معکوس خود را از طریق Baidu، TinEye، Yandex، Google و Bing انجام دهند. بهتر است همیشه از چند موتور جستجوی مختلف استفاده کنید چراکه نتایج آن‌ها اغلب با یکدیگر متفاوت است.

اگر سایت یا اکانت مورد نظر متنی را به اشتراک گذاشته باشد، می‌توانید جستجو کنید و ببینید آن متن در چه جاهای دیگری ظاهر شده است. در مورد متون طولانی‌تر، توصیه می‌شود یک یا دو جمله از پاراگراف‌های سوم یا چهارم یا پایین‌تر انتخاب کنید، چون در عملیات‌های گمراه‌سازی تغییر دادن سرتیترها و پاراگراف‌های ابتدایی حقه‌ی رایجی است، اما احتمال کمتری وجود دارد که برای تغییر دادن بدنه‌ی مقاله نیز وقت صرف شود. قرار دادن بخش انتخاب‌شده در علامت نقل قول در جستجوی گوگل، نتایجی با مطابقت دقیق را نشان خواهد داد. با استفاده از منوی "Tools" می‌توانید نتایج را به ترتیب تاریخ مرتب کنید.



نتایج جستجوی گوگل برای عبارتی که توسط حسابی مشکوک به ارتباط با عملیات روسیه ارسال شده است، که عملکرد ابزار گوگل را برای محدود کردن تاریخ جستجو نشان می‌دهد.

سایت‌ها و اکانت‌هایی که متنی حاوی اشتباه املایی ارسال می‌کنند ارزش خاصی دارند، زیرا اشتباهات طبیعتا غیررایج‌تر از کلماتی هستند که به درستی نوشته می‌شوند. به‌عنوان مثال، در مقاله‌ای مشکوک به ارتباط با عملیات اطلاعاتی روسیه نام شهر

سالزبری، شهری که سرگئی اسکریپال مأمور سابق روسیه در آن مسموم شده بود، به جای املای صحیح یعنی "Salisbury" از املای "Solsbury" استفاده شده بود. همین امر باعث شد به جای جستجوی کلمات "Salisbury"و "Skripal" که بسیار عام بودند و نتایج بسیار زیادی را به دست می‌دادند، جستجوی هدفمندتری صورت بگیرد و نتایج کمتر اما دقیق‌تری به دست بیاید.

در خصوص سرنخ‌های مربوط به محتوا، توجه به شاخص‌های دیگر مانند الگوی فعالیت‌ها برای تأیید اینکه آیا آن سایت یا اکانت به یک عملیات تعلق دارد یا خیر بسیار مهم است. کاربران ممکن است به دلایل موجه بسیاری محتوای تولیدشده توسط یک عملیات گمراه‌سازی یا دروغ‌پراکنی را بازنشر کنند. این یعنی اشتراک‌گذاری یک محتوا تنها می‌تواند سرنخ ضعیفی برای محققان باشد. برای مثال، بسیاری از کاربران میم‌های آژانس تحقیقات اینترنتی روسیه را به اشتراک گذاشته‌اند، زیرا آن میم‌ها دارای ویژگی‌هایی بودند که آن‌ها را بسیار پربازدید و پرکاربرد می‌کرد. صرف به اشتراک گذاشتن محتوا نمی‌تواند دلیل کافی برای دست داشتن در یک عملیات باشد.

جمع‌آوری شواهد

عملیات اطلاعاتی و تأثیرگذاری دارای ماهیتی پیچیده هستند و به‌سرعت پیش می‌روند. یکی از ناامیدکننده‌ترین تجربیات برای یک محقق منبع باز، این است که ببیند مجموعه‌ای از دارایی‌ها در نیمه‌راه تحقیق از فضای آنلاین حذف شده و از دسترس خارج می‌شوند. بنابراین، یک قانون کلیدی در تحقیقات این است که مادامی که به شواهد دسترسی دارید باید آن‌ها را ثبت کنید، زیرا ممکن است شانس دومی به دست نیاورید.

محققان مختلف ترجیحات متفاوتی برای ثبت داشته‌ها دارند و نیازها نیز ممکن است از عملیاتی به عملیات دیگر متفاوت باشند. صفحات گسترده برای ثبت اطلاعات اولیه در مورد تعداد زیادی از داشته‌ها مفید هستند. برای ذخیره کردن اسکرین‌شات‌ها می‌توان از فضاهای ذخیره‌سازی ابری استفاده کرد. (در خصوص اسکرین‌شات‌ها بهتر است بلافاصله از پوشه‌های مجزا با نام‌های خاص و قابل شناسایی استفاده کنید. هیچ چیز آزاردهنده‌تر از گشتن به دنبال عکسی خاص در میان انبوهی از پوشه‌ها که همگی نام اسکرین‌شات را بر خود دارند نیست). اسناد متنی برای ضبط ترکیبی از اطلاعات

مناسبند، اما اگر عملیات بزرگ باشد به سرعت درهم و برهم می‌شوند و استفاده از اطلاعات ثبت‌شده در آن‌ها دشوار می‌شود.

از هر فرمتی که استفاده می‌کنید به خاطر داشته باشید برخی اطلاعات هستند که همیشه باید ثبت شوند. از جمله اینکه سایت یا حساب کاربری مورد نظر چگونه شناسایی شده (یک نکته‌ی کاملا ضروری)، نام و URL آن، تاریخ ایجاد (در صورتی که موجود باشد)، تعداد دنبال‌کنندگان، تعداد کسانی که توسط آن دنبال می‌شوند و همینطور تعداد لایک‌ها و بازدیدها. همچنین، اضافه کردن توضیحی اجمالی درباره‌ی سایت یا حساب کاربری نیز ضروری است (به‌عنوان مثال، حساب کاربری به زبان عربی حامی عربستان سعودی که از عکس اما واتسون به‌عنوان تصویر پروفایل خود استفاده کرده است). این کار کمکتان خواهد کرد بعد از بازدید از تعداد زیادی حساب کاربری داشته‌ی مورد نظر را به یاد بیاورید. اگر به صورت گروهی کار می‌کنید، شاید بد نباشد در توضیحات خود ذکر کنید که هر کس روی کدام سایت یا حساب کاربری کار کرده است.

لینک‌ها را می‌توان با استفاده از یک سرویس بایگانی مانند Wayback Machine یا archive.is حفظ کرد، اما مراقب باشید که این بایگانی‌ها هویت کاربران واقعی‌ای را که ممکن است ناخواسته با داشته‌های مشکوک تعامل داشته باشند، افشاء نکنند و مطمئن شوید لینکی که ذخیره کرده‌اید شامل تصاویر هم می‌شود و یا برای اطمینان خاطر از تصاویر اسکرین‌شات بگیرید. اطلاعات مربوط به داشته‌ها را در فضاهای محافظت‌شده، مانند فایل‌های دارای رمز عبور و یا فضاهای ذخیره‌سازی رمزنگاری‌شده، ذخیره کنید. همیشه فهرست افرادی که به منابع دسترسی دارند و آخرین دسترسی‌ها را بررسی کنید.

درنهایت، می‌توانید به سایت‌ها و حساب‌های کاربری که شناسایی کرده‌اید امتیاز اطمینان بدهید. عملیات‌های گمراه‌سازی اغلب از کاربران ناآگاهی که ناخواسته محتوای آن‌ها را تقویت می‌کنند استفاده می‌کنند: در واقع، اغلب هدف همین است. چقدر مطمئن هستید که آخرین دارایی شناسایی‌شده بخشی از این عملیات است و چرا؟ سطح اطمینان (بالا، متوسط یا پایین) باید به‌عنوان یک ورودی جداگانه درج شود و دلایل (که در ادامه درباره‌ی آن‌ها بحث خواهد شد) باید به یادداشت‌ها اضافه شوند.

انتساب و اطمینان

بزرگترین چالش شناسایی یک عملیات اطلاعاتی نسبت دادن آن به یک عامل خاص است. در بسیاری از موارد، انتساب عملیات به یک عامل دقیق از محققین منبع‌باز ساخته نیست. گاهی بهترین نتیجه‌ای که می‌توان به دست آورد این است که تا حدی با اطمینان بگوییم یک عملیات احتمالا توسط یک بازیگر خاص اداره می‌شود، یا اینکه داشته‌های خاصی به یک عملیات خاص تعلق دارند، اما تعیین اینکه چه کسی پشت یک عملیات است به ندرت با منابع باز امکان‌پذیر است.

اطلاعاتی مانند ثبت دامنه‌ی وبسایت‌ها، آدرس‌های IP و شماره تلفن‌ها می‌توانند یک منبع متقن ارائه دهند، اما اغلب دسترسی به این اطلاعات به جز برای پلت‌فرم‌های رسانه‌های اجتماعی برای کس دیگری امکان‌پذیر نیست. به همین دلیل است که تماس با پلتفرم‌های مربوطه بخش مهمی از کار تحقیقاتی است. بیشترین انتساب‌ها در موارد اخیر مستقیما توسط خود پلتفرم‌ها صورت گرفته است، مانند افشای عملیات اطلاعاتی تحت حمایت دولت چین که هنگ‌کنگ را هدف قرار می‌داد توسط توئیتر، و یا افشای عملیات‌های مرتبط با دولت عربستان سعودی توسط فیس‌بوک.

سرنخ‌های موجود در محتوا می‌توانند نقش مهمی داشته باشند. به‌عنوان مثال، عملیاتی که در اکتبر ۲۰۱۹ در اینستاگرام افشا شد، میم‌هایی را منتشر کرده بود که تقریبا با میم‌های ارسال‌شده توسط آژانس تحقیقات اینترنتی روسیه یکسان بود، اما واترمارک آن‌ها حذف شده بود. تنها راه ساختن این میم‌ها این بود که تصاویر اصلی را که مبنای پست‌های آی‌آرای بود تهیه کنند و سپس میم‌ها را روی آن‌ها بازسازی کنند. از قضا، این تلاش برای پنهان کردن منشأ پست‌های آی‌آرای نشان می‌داد که مبتکر آن درواقع خود آی‌آرای بوده است.

به‌همین‌ترتیب، شبکه‌ی بزرگی از وب‌سایت‌های به‌ظاهر مستقل، مکررا مقالاتی را منتشر کرده بودند که بدون ذکر منبع، از منابع دولتی ایران کپی شده بودند. این الگو به‌قدری تکرار شده بود که نشان داد فعالیت اصلی وب‌سایت‌ها درواقع همین بوده است. به‌این‌ترتیب، می‌توان این عملیات را به عاملان حامی ایران نسبت داد، اما نمی‌توان از آن فراتر رفت و عملیات را به خود دولت ایران نسبت داد.

و در آخر اینکه، نکته‌ی مهم در مسئله‌ی انتساب، خویشتنداری است. محقق باید این سوال را از خود بپرسد: «چگونه می‌توان ثابت کرد که این عملیات توسط شخصی که متهمش می‌کنیم انجام شده

است؟» و در صورتی که نمی‌تواند با اطمینان به این سؤال پاسخ دهد، باید از متهم کردن فرد مذکور خودداری کنند. شناسایی و افشای یک عملیات اطلاعاتی کار دشوار و مهمی است و یک انتساب بدون پشتوانه یا نادرست می‌تواند ارزش همه‌ی کارهای مهمی را که تا آن مرحله انجام شده زیر سوال ببرد.

۱۱.الف. مطالعه‌ی موردی: انتساب عملیات اِندلِس مِی‌فلای

نوشته‌ی: **گابریل لیم**

گابریل لیم محقق پروژه‌ی تحقیقاتی فناوری و تغییرات اجتماعی در مرکز شورنستاین مدرسه‌ی کندی هاروارد و یکی از همکاران سیتیزن لب است. او پیامدهای سانسور و دستکاری رسانه‌ها را بر امنیت و حقوق بشر مطالعه می‌کند.

در آوریل ۲۰۱۷، یک مقاله‌ی جعلی که تظاهر شده بود در خبرگزاری بریتانیایی معتبر ایندیپندنت چاپ شده در ردیت پست شد. این مقاله به دروغ از نیک کلِگ، که آن زمان معاون نخست‌وزیر بود، نقل کرده بود که ترزا می، نخست‌وزیر وقت، «چاپلوسی دولت‌های عربی را می‌کند». کاربران باهوش ردیت بلافاصله به این پست مشکوک شدند و توجه‌ها را به نادرستی آن جلب کردند. مقاله نه‌تنها به جای www.independent.co.uk روی وب‌سایتی با آدرس indepnedent.co منتشر شده بود، بلکه ارسال‌کننده‌ی اصلی آن نیز یک شخصیت سطحی بود که چند مقاله‌ی جعلی دیگر از این دست نیز در ردیت پست کرده بود.

تحقیقات از آن مقاله، دامنه‌ی وب و شخصیت ساختگی آغاز شد و محققان سیتیزن لب ۲۲ ماه بعد را صرف ردیابی و تحقیق در مورد شبکه‌ای کردند که پشت این عملیات اطلاعاتی چندوجهی پنهان شده بود. این عملیات، که اِندلِس مِی‌فلای (Endless Mayfly) نام گرفته بود، قصد داشت با هدف قرار دادن روزنامه‌نگاران و فعالان به وسیله‌ی وب‌سایت‌های ساختگی‌ای که شبیه به وب‌سایت‌های معتبر طراحی شده بودند، اطلاعات نادرست و تفرقه‌افکنانه منتشر کند.

روش کار کلی عملیات به این شکل بود که مقالاتی جعلی را با تقلید نام خبرگزاری‌های معتبر توسط مجموعه‌ای از وب‌سایت‌ها و شخصیت‌های توئیتری پخش می‌کرد و به محض اینکه محتوا سروصدای مورد نظر را در فضای مجازی ایجاد می‌کرد، مقاله را حذف کرده یا نشانی وب آن را تغییر می‌داد. در زیر نمونه‌ای از این مقاله‌ها را که با استفاده از خطای عمدی در نشانی وب، منتسب به خبرگزاری بلومبرگ جا زده شده است را مشاهده می‌کنید (به جای نشانی Bloomberg.com از bloomberq.com

استفاده شده است):

تصویر زیر دو شخصیت آنلاین جعلی وابسته به اندلس می‌فلای را نشان می‌دهد که لینکی متصل به نسخه‌ی تقلیدی از روزنامه‌ی دِیلی صباح، از خبرگزاری‌های ترکیه، را توئیت کرده‌اند. توجه داشته باشید که شخصیت سمت راست، jolie prevoit از عکس بازیگری به نام الیشا کاتبرت به‌عنوان عکس پروفایل خود استفاده کرده است.

تا زمانی که گزارش خود را در ماه مه ۲۰۱۹ منتشر کردیم، مجموعه داده‌های ما شامل ۱۳۵ مقاله‌ی غیرمعتبر، ۷۲ دامنه، ۱۱ شخصیت، یک سازمان جعلی و یک شبکه‌ی نشر طرفدار ایران بود که اطلاعات نادرست موجود در مقالات غیرمعتبر را تقویت می‌کرد. در پایان، با اطمینان متوسط به این نتیجه رسیدیم که اندلس می‌فلای یک عملیات اطلاعاتی همسو با ایران است.

مثال اندلس می‌فلای نشان می‌دهد که چگونه می‌توانید تحلیل شبکه و تحلیل روایی را با گزارش‌های خارجی ترکیب کنید تا بتوانید عملیات را به عامل خاصی منتسب کنید. این نمونه همچنین دشواری‌های نسبت دادن عملیات اطلاعاتی به یک بازیگر خاص، چرایی نیاز به چند شاخص و نحوه‌ی استفاده از شاخص سطح اطمینان برای نشان دادن میزان اطمینان از انتسابی که انجام داده‌اید را نیز برجسته می‌کند.

درنهایت، انتساب کاری دشوار است که اغلب نقص‌های اطلاعات امکان انجام آن را محدود می‌کند، مگر اینکه بتوانید از عاملان اعتراف صریح بگیرید و یا مدرکی یقینی برای اثبات ادعای خود داشته باشید. به همین دلیل است که در بسیاری از مواردِ دستکاری رسانه‌ها انتساب اغلب به صورت یک تخمین احتمالی بیان می‌شود.

مثلث‌بندی نقاط داده و تحلیل

با توجه به ماهیت مخفیانه‌ی عملیات اطلاعاتی، امکان استفاده‌ی عاملان از استراتژی پرچم دروغین (false flag) و همچنین ماهیت موقتی شواهد، هر انتسابی باید با کمک ترکیبی از تحلیل و شواهد صورت بگیرد. در خصوص اندلس می‌فلای، ما با اطمینان متوسط به این نتیجه رسیدیم که این عملیاتی همسو با ایران است، و برای رسیدن به این نتیجه از شاخص‌هایی که از سه نوع تحلیل به دست می‌آیند استفاده کردیم:

۱. تحلیل روایی

۲. تجزیه و تحلیل شبکه

۳. گزارش و تحلیل خارجی

۱. تحلیل روایی

با استفاده از تحلیل محتوا و گفتمان بر روی ۱۳۵ مقاله‌ی غیرمعتبری که در تحقیقات جمع‌آوری شده بودند، به این نتیجه رسیدیم که روایت‌های منتشرشده با منافع ایران همسو هستند. پس از مطالعه‌ی اولیه، تمام مقالات را در دسته‌بندی‌های خاصی که ایجاد کرده بودیم گنجاندیم. تقسیم‌بندی مقالات در دو دور مجزا صورت گرفت: در دور اول، دو محقق هر کدام به صورت مستقل مقاله‌ها را مطالعه و تقسیم‌بندی کردند. در دور دوم دو محقق برای برطرف کردن مغایرت‌های موجود تقسیم‌بندی را با همکاری هم انجام دادند. جدول زیر نتیجه‌ی این تقسیم‌بندی‌ها را نشان می‌دهد:

Category	Article count	Category description
Geopolitical discord	63 (46.7%)	The article describes events, actions or statements made by government officials toward a foreign state that may be construed as provocative, hostile or counter to the foreign state's interests.
Domestic discord	16 (11.9%)	The article describes events, actions or statements made by political actors that may sow discord between political parties or actors within the same state.
Cooperating with Israel	14 (10.4%)	The article describes events, actions or statements made by political actors or government officials that show cooperation between Israel and another state.
Saudi Arabia supports terrorism	9 (6.7%)	The article describes events, actions or statements that either link Saudi Arabia to terrorist activity or allege that Saudi Arabia supports terrorism.
Other	5 (3.7%)	The article does not fit into any of the categories.
No archive	31 (23%)	The article cannot be coded because it no longer exists and there is no cache, screenshot or copy of the text to perform any meaningful analysis.
Copy of existing article	5 (3.7%)	The article is a direct copy/paste of an already existing real article.

پس از تقسیم‌بندی مقالات موفق شدیم رایج‌ترین روایت‌های منتشرشده توسط اندلس می‌فلای را مشخص کنیم. سپس نتایج را با تحقیقات اولیه‌ای که درباره‌ی منطقه انجام داده بودیم مقایسه کردیم. این شامل تحقیقاتی گسترده برای درک رقابت‌ها و اتحادهای منطقه، منافع و تهدیدات ژئوپلیتیکی و تاریخچه‌ی کنترل‌های اطلاعاتی بود. این کار برای قرار دادن و درک اطلاعات در بستر و زمینه‌ی سیاسی گسترده‌تر ضروری بود. درنهایت ، با بررسی خروجی تحقیقات به این نتیجه رسیدیم این روایات به احتمال زیاد در خدمت منافع ایران هستند.

۲. تجزیه و تحلیل شبکه

تجزیه و تحلیل شبکه به این منظور صورت گرفت که بفهمیم چه دامنه‌ها یا پلتفرم‌هایی در تقویت محتوای مورد نظر نقش داشته‌اند. دو شبکه در انتشار مقالات غیرمعتبر و دروغ‌های اندلس می‌فلای دست داشتند: شبکه‌ای از وب‌سایت‌های حامی ایران، و مجموعه‌ای از شخصیت‌های طرفدار ایران در توئیتر. هر دوی این‌ها در تصمیم ما برای انتساب عملیات اندلس می‌فلای به ایران نقش داشتند، چراکه به طور مداوم داستان‌هایی را که با سیاست‌ها، بیانیه‌های عمومی و مواضع ایران در رابطه با عربستان سعودی، اسرائیل و ایالات متحده مطابقت دارد منتشر می‌کنند.

شبکه‌ی نشر: شبکه‌ی انتشار متشکل از تعدادی وب‌سایت حامی ایران بود که خود را به‌عنوان رسانه‌های خبری مستقل معرفی می‌کردند. در مجموع، ما ۳۵۳ وب‌سایت را در ۱۳۲ دامنه پیدا کردیم که به مقالات غیرمعتبر اندلس می‌فلای ارجاع یا لینک داده بودند. این فرآیند شامل جستجوی URL همه‌ی مقالات غیرمعتبر و عناوین آن‌ها در گوگل بود. علاوه‌براین، ما لینک‌های توئیت‌شده توسط شخصیت‌های مرتبط با شبکه را نیز بررسی کردیم و وب‌سایت‌هایی را که حاوی ارجاعات یا لینک‌هایی به مقالات بودند را شناسایی کردیم.

با استفاده از این روش ما ۱۰ دامنه‌ای را که بیشتر از همه به مقالات غیرمعتبر ارجاع داده بودند شناسایی کردیم. از این ۱۰ دامنه ۸ تا آدرس IP یا جزئیات ثبت یکسانی داشتند که نشان می‌داد ممکن است توسط یک عامل کنترل شوند. محتوای این وب‌سایت‌ها نیز عمدتا در حمایت از منافع ایران بود. به‌عنوان مثال، IUVM Press که ۵۷ بار به مقالات غیرمعتبر اندلس می‌فلای لینک یا ارجاع داده است، یک سند پی‌دی‌اف با عنوان «اساسنامه» را میزبانی کرده است که به صراحت اعلام می‌کند مخالف

«فعالیت‌ها و پروژه‌های کشورهای استکبار جهانی، امپریالیسم و صهیونیسم» است و در آن تصریح شده که مقر اتحادیه در تهران، پایتخت جمهوری اسلامی ایران قرار دارد.

شبکه‌ی شخصیت‌های توئیتری: مانند مقالات غیرمعتبر و شبکه‌ی نشر، شخصیت‌های وابسته به اندلس می‌فلای در توئیتر نیز قاطعانه از عربستان سعودی، اسرائیل و به‌طور کلی کشورهای غربی انتقاد می‌کردند. تجزیه و تحلیل فعالیت آن‌ها در توئیتر نشان داد که این حساب‌ها ترکیبی از مقالات معتبر و غیرمعتبر را منتشر می‌کنند که در آن‌ها به‌شدت از رقبای سیاسی ایران انتقاد شده است. به‌عنوان مثال، حساب توئیتر «انجمن صلح، امنیت، عدالت» را در نظر بگیرید؛ سازمانی جعلی که توسط گروه تحقیقاتی ما شناسایی شد و در زیر نشان داده شده است. این حساب نه‌تنها محتواهایی که بر ضد عربستان سعودی، اسرائیل و ایالات متحده بود را نشر و تبلیغ می‌کند، بلکه عکس پروفایل و تصویر بالای صفحه‌ی کاربری آن نیز عربستان سعودی را هدف قرار می‌دهد. بیوگرافی این حساب نیز به‌صراحت عربستان سعودی و ایدئولوژی وهابی را عامل افراط گرایی قلمداد می‌کند.

به‌همین‌ترتیب، این توئیت از یکی دیگر از شخصیت‌های اندلس می‌فلای به نام مونا آ. رحمان، ضمن انتقاد از محمد بن سلمان، ولیعهد عربستان سعودی، از علی الاحمد، روزنامه‌نگار و منتقد سعودی یاد می‌کند.

۳. گزارش و تحلیل خارجی

ما همچنین یافته‌ها و داده‌های خود را با گزارش‌های خارجی نیز مقایسه کردیم. به‌عنوان مثال، به دنبال هشداری از طرف فایر آی در آگوست ۲۰۱۸، فیس‌بوک برخی از حساب‌ها و صفحات مرتبط با شبکه‌ی نشر اندلس می‌فلای را غیرفعال کرده بود. فایر آی در تجزیه و تحلیل خود چندین دامنه، از جمله institutomanquehue.org و RPFront.com، را شناسایی کرده بود که بخشی از همان شبکه‌ی نشری بودند که ما نیز شناسایی کرده بودیم. آن‌ها نیز مانند ما با اطمینان متوسط به این نتیجه رسیده بودند که ظاهرا «عملیات تأثیرگذاری مورد نظر» از ایران سرچشمه می‌گیرد. فیس‌بوک نیز در اطلاعیه‌ی خود اعلام کرد که عملیات احتمالا از ایران نشأت می‌گیرد.

علاوه‌براین، توئیتر نیز مجموعه‌داده‌ای از حساب‌های مرتبط با ایران را منتشر کرده بود که به دلیل «دستکاری هماهنگ اطلاعات» تعلیق شده بودند. اگرچه حساب‌هایی که در زمان تعلیق کمتر از ۵ هزار دنبال‌کننده داشتند ناشناس نگه داشته شده بودند، ما توانستیم یک شخصیت اندلس می‌فلای با نام کاربری@Shammari_Tariq را در مجموعه‌داده‌ی توئیتر شناسایی کنیم.

ارزیابی‌های توئیتر، فیس‌بوک و فایر آی در تأیید فرضیه‌ی ما مفید بودند، زیرا شواهدی را به دست می‌دادند که ما در تلاش‌های خود برای جمع‌آوری داده موفق به کشف آن‌ها نشده بودیم و درعین‌حال، با دارایی‌های اندلس می‌فلای که ما شناسایی کرده بودیم همپوشانی داشتند. به‌عنوان مثال، تجزیه و تحلیل فایر آی شامل شماره‌ی تلفن و اطلاعات ثبت حساب‌های توئیتر و دامنه‌های مرتبط با اندلس می‌فلای بود - شواهدی که بخشی از مجموعه‌داده‌ی ما نبودند. به‌همین‌ترتیب، فیس‌بوک و توئیتر به اطلاعاتی مانند اطلاعات ثبت حساب کاربری، ازجمله آدرس‌های IP، دسترسی داشتند که دسترسی به آن‌ها برای ما مقدور نیست. بنابراین، نقاط داده‌ی شناسایی شده توسط این گزارش‌های خارجی به گسترش مجموعه‌ی شواهد ما کمک شایانی کرد.

رسیدن به سطح اطمینان متوسط

در پروژه‌ی تحقیقاتی اندلس می‌فلای شواهدی که موفق به جمع‌آوری‌شان شدیم - روایت‌ها، شخصیت‌ها و شبکه‌های نشر حامی ایران - به ایران به‌عنوان منبع احتمالی عملیات اطلاعاتی اشاره داشتند. این مجموعه شواهد سپس با گزارش‌ها و تحقیقات خارجی معتبر از فایر آی، فیس‌بوک و توئیتر مقایسه شد که نتایج ما را تأیید می‌کردند. اگرچه هر یک از شواهد به تنهایی برای انتساب کافی نیستند، با دیدی کل‌نگر و با مقایسه‌ی مجموع شواهدی که از تحقیقات مختلف به دست آمده بود، شواهد به تأیید فرضیه‌ی ما کمک می‌کردند.

علی‌رغم عناصر متعددی که به دست داشتن ایران در این عملیات اشاره داشتند، هنوز دلیل متقنی برای اثبات این فرضیه در دست نداشتیم. به همین دلیل از چارچوب رایج جامعه‌ی اطلاعاتی برای انتساب عملیات در فضای مجازی استفاده کردیم. این چارچوب از شاخص‌های چندگانه و احتمالی میزان اطمینان (کم، متوسط، زیاد) استفاده می‌کند و به محققان این امکان را می‌دهد که نتایج خود را با مشخص کردن میزان قطعیت منتشر کنند.

درنهایت، ما به این نتیجه رسیدیم که اندلس می‌فلای عملیاتی همسو با ایران و با درجه‌ی اطمینان متوسط است که بنا به تعریف اداره‌ی اطلاعات ملی ایالات متحده به این معنی است که «اطلاعات قابل پذیرش و دارای منابع قابل‌قبول هستند اما کیفیت لازم یا شواهد کافی برای اختصاص دادن

درجه‌ی بالاتری از اطمینان را دارا نیستند». دلیل خودداری ما از در نظر گرفتن سطح بالاتری از اطمینان این بود که احساس کردیم شواهد کافی را برای رد امکان‌های دیگر -از جمله اینکه عملیات درواقع نوعی عملیات پرچم دروغین (به این معنی که عامل دیگری در تلاش باشد وانمود کند عملیات توسط ایران اداره می‌شود) باشد و یا توسط عامل سومی اداره شود که از منافع ایران حمایت می‌کند- در دسترس نداریم.

نسبت دادن عملیات اطلاعاتی‌ای مانند اندلس می‌فلای در اکثر مواقع بر اطلاعات ناقص و محدود متکی خواهد بود. بنابراین، استفاده از شاخص سطح اطمینان، که نشانگر به کار بستن احتیاط‌های لازم است، عنصر مهمی در عمل انتساب است. انتساب نادرست یا سطح اطمینان بیش از حد بالا می‌تواند عواقب بدی داشته باشد، خصوصا اگر انتساب نادرست سیاست‌های خاص دولت و اقدامات تلافی‌جویانه را در پی داشته باشد. برای پرهیز از انتساب‌های عجولانه و ضعیف، مهم است که چندین شاخص مختلف، انواع شواهد و تحلیل‌ها را در نظر بگیرید و از سطح اطمینانی استفاده کنید که فرضیه‌های جایگزین و داده‌های غایب نیز در آن لحاظ شده باشند.

۱۱.ب. مطالعه‌ی موردی: بررسی یک عملیات اطلاعاتی در استان پاپوآی غربی

نوشته‌ی: **الیز توماس، بنجامین استریک**

بنجامین استریک به‌عنوان محقق منبع‌باز با بی‌بی‌سی، و به‌عنوان نویسنده با بلینگ‌کت همکاری می‌کند و مدرس تکنیک‌های منبع‌باز، اطلاعات مکانی (geospatial) و تحلیل شبکه نیز هست. او تجربیاتی در رشته‌ی حقوق و در ارتش داشته و در حال حاضر بر استفاده از روش‌های اطلاعات منبع‌باز/اطلاعات مکانی، موقعیت جغرافیایی و عملیات اطلاعاتی برای اهداف مثبت از جمله حقوق بشر، درگیری‌ها و حفظ حریم خصوصی تمرکز دارد.

الیز توماس روزنامه‌نگار مستقل و محققی است که با مرکز بین‌المللی سیاست سایبری در مؤسسه‌ی سیاست استراتژیک استرالیا کار می‌کند. نوشته‌های او در وایِرد، فارن پالیسی، دیلی بیست، گاردین و سایر رسانه‌ها منتشر شده است. او همچنین پیش از این به‌عنوان دستیار تحریریه در دفتر هماهنگی امور بشردوستانه‌ی سازمان ملل متحد و نیز به‌عنوان نویسنده و مجری پادکست فعالیت کرده است.

در آگوست ۲۰۱۹، تنش‌های جدایی‌طلبانه بار دیگر در پاپوآی غربی -استانی که در دهه‌ی ۱۹۶۰ و در پی تصمیمی بحث‌انگیز به اندونزی الحاق شد- بالا گرفت. از آن زمان تاکنون، دولت اندونزی بارها برای سرکوب مخالفان در منطقه متهم به نقض گسترده‌ی حقوق بشر شده است.

دسترسی به این منطقه به‌شدت محدود شده و خبرنگاران خارجی از گزارش کردن در این استان منع شده‌اند. همه‌ی اینها باعث شده رسانه‌های اجتماعی به منبعی حیاتی برای رصد و گزارش رویدادها در پاپوآی غربی تبدیل شوند.

درحالیکه سعی داشتیم ویدئوهایی را که از خشونت‌ها در فَک‌فَک (FakFak) در پاپوآی غربی منتشر شده بود مکان‌یابی کنیم، یکی از ما موفق به کشف دو هشتگی شد که در توئیتر در حال انتشار بودند: #FreeWestPapua و #WestPapua.

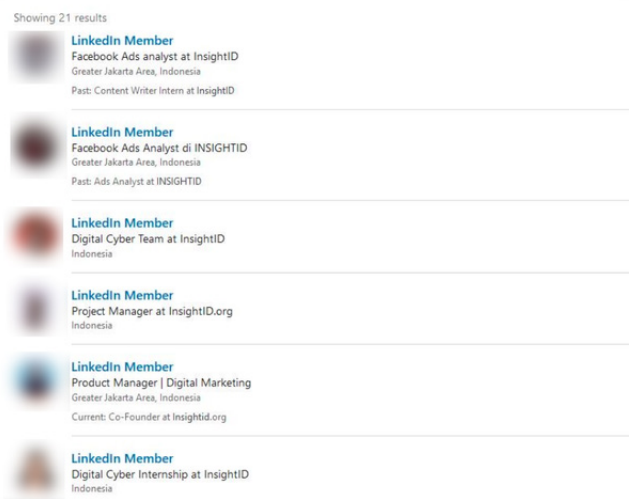
جستجوی این هشتگ‌ها موجی از حساب‌های جعلی را نشان داد که با استفاده از این هشتگ‌ها،

ویدئوها و متن‌های یکسانی را به صورت خودکار ارسال می‌کردند. این حساب‌ها همچنین محتوای یکدیگر را بازتوئیت و لایک می‌کردند و از این طریق به تقویت بیشتر هشتگ‌ها و افزایش تعامل آن‌ها کمک می‌کردند.

روند تجزیه و تحلیل این حساب‌های خودکار در فصل سه به تفصیل شرح داده شد. با تکیه بر کاری که برای شناسایی حساب‌ها صورت گرفته بود، ما تحقیقات خود را گسترش داده و تلاش کردیم افراد و گروه‌هایی را که پشت این عملیات گسترده بودند شناسایی کنیم. در این روند ما موفق به کشف کمپینی کوچک‌تر و به‌ظاهر بی‌ارتباط با کمپین اول شدیم و همچنین توانستیم فرد مسئول را نیز شناسایی کنیم. گردانندگان هر دو کمپین درنهایت پس از تماس بی‌بی‌سی به دخالت خود اعتراف کردند.

بزرگی کمپین اول و این واقعیت که در چندین پلتفرم مختلف فعالیت می‌کرد، به ما این فرصت را داد تا سرنخ‌هایی را پیدا کنیم که ما را به سمت اطلاعات بیشتر درباره‌ی گرداننده‌ی کمپین راهنمایی کند.

اولین اطلاعات مفید وب‌سایت‌هایی بودند که توسط شبکه‌ی حساب‌ها در توئیتر و فیس‌بوک به اشتراک گذاشته می‌شدند. جستجوهای Whois نشان داد که ۴ دامنه با نام جعلی و آدرس ایمیل ساختگی، اما با یک شماره تلفن واقعی ثبت شده‌اند. ما شماره را در واتس‌اپ وارد کردیم تا ببینیم آیا به حساب کاربری‌ای متصل است یا خیر. پاسخ مثبت بود و آن حساب یک عکس پروفایل نیز داشت.



با استفاده از جستجوی معکوس عکس پروفایل در Yandex توانستیم عکس پروفایل را به حساب‌هایی در فیس‌بوک، لینکدین و Freelancer.com متصل کنیم. از طریق حساب لینکدین مرتبط، توانستیم محل کار فعلی فرد را پیدا کرده و ببینیم همکارانش چه کسانی هستند.

این فرد کارمند شرکتی مستقر در جاکارتا به نام اینسایت آی‌دی بود که به گفته‌ی وب‌سایت شرکت کار آن ارائه‌ی «برنامه‌های جامع روابط عمومی و بازاریابی دیجیتال» است.

ما همچنین موفق به جمع‌آوری نقاط داده‌ی دیگری شدیم که نشان می‌داد اینسایت آی‌دی مسئول عملیات اطلاعاتی است. اینسایت آی‌دی در وب‌سایت خود به فعالیت‌هایش در «طرح‌های توسعه در پاپوآ» اشاره کرده و ادعا کرده بود که «توسعه‌ی سریع اجتماعی‌اقتصادی در پاپوآ و چالش‌های آن را بررسی می‌کند». کارمندان و کارآموزان سابق اینسایت آی‌دی تولید محتوای ویدئویی، نوشتن مطالب تبلیغاتی و ترجمه‌ی محتوا را بخشی از کار خود در پروژه‌ی توسعه‌ی پاپوآ توصیف کرده بودند.

یکی از کارمندان سابق در پروفایل لینکدین خود اشاره کرده بود که کار آن‌ها را می‌توان در West Papuan (اینستاگرام، فیس‌بوک، وب‌سایت) مشاهده کرد. West Papuan یکی از وب‌سایت‌های خبری درگیر در این کمپین بود. یکی دیگر از کارمندان اینسایت آی‌دی یک حساب یوتیوب به نام خود ایجاد کرده بود تا ویدئویی را که بخشی از کمپین بود با استفاده از آن منتشر کند. این ویدئو سپس در westpapuan.org جاگذاری شده بود.

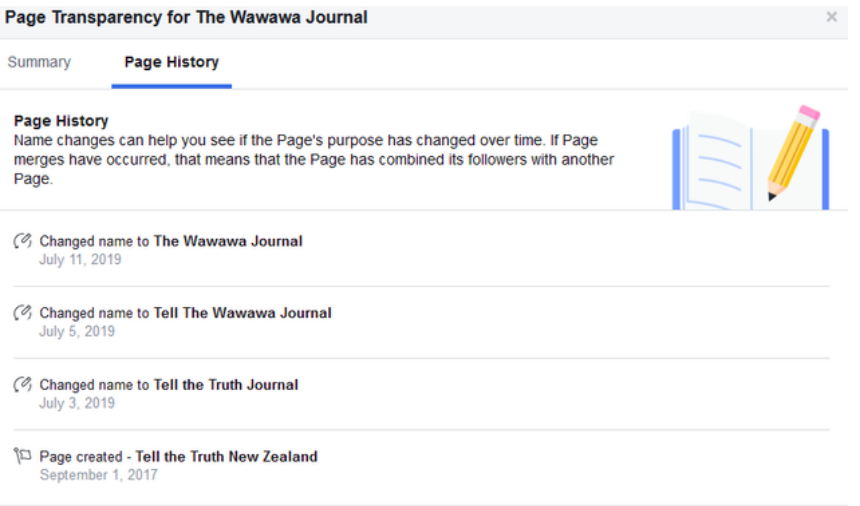
جستجوهای بیشتر در سوابق ثبت دامنه نشان داد که یکی از بنیانگذاران اینسایت آی‌دی با استفاده از آدرس ایمیل شرکت خود ۱۴ دامنه در یک روز ثبت کرده است که بیشترشان به‌وضوح و مستقیما به پاپوآی غربی مربوط می‌شدند.
این دامنه‌ها شـامل westpapuagenocide.com، westpapuafreedom.com و westpapuafact.com بودند. هر اطلاعات جدیدی که به شواهد اضافه می‌شد، ظن ما را در این مورد که اینسایت آی‌دی مسئول عملیات بوده است بیشتر می‌کرد.

در آن زمان، خبرنگاران بی‌بی‌سی تلاش کردند با اینسایت آی‌دی تماس بگیرند و نظر آن‌ها را در این مورد بشنوند. اگرچه شرکت در این تماس تلفنی پاسخی نداد، اما درنهایت مسئولیت خود را پذیرفت و در یک پست رسانه‌ی اجتماعی اذعان کرد که «محتوای ما از اندونزی در برابر روایات جعلی گروه‌های جدایی‌طلب Free Papua دفاع می‌کند».

ما موفق به شناسایی شخصی که اینسایت آی‌دی را برای انجام این عملیات اطلاعاتی استخدام کرده بود نشدیم.

در همان حین که مشغول بررسی این عملیات بزرگ بودیم، موفق به کشف عملیات کوچک‌تری شدیم شامل سه وب‌سایت که خود را وب‌سایت‌های خبری مستقل معرفی می‌کردند و حساب‌های کاربری مرتبط با خود را در شبکه‌های اجتماعی داشتند. این سایت‌ها اگرچه ظاهرا به کمپین اول متصل نبودند، اما برداشت‌های بین‌المللی از وضعیت پاپوآی غربی را هدف قرار داده بودند و بر مخاطبان در نیوزلند و استرالیا تمرکز داشتند.

کلید شناسایی فرد مسئول در این کمپین این بود که صفحه‌ی فیس‌بوک یکی از برندها، مجله‌ای به نام Wawawa، در ابتدا Tell the Truth NZ نام داشت. ما با بررسی سوابق نام‌گذاری صفحه موفق به کشف این نام قدیمی شدیم. این به ما امکان داد دامنه‌ی مرتبط با نام قبلی یعنی tellthetruthnz.com را پیدا کرده و کمپین را با فردی به نام محمد روزید جزولی که این دامنه را ثبت کرده بود پیوند دهیم.
هنگامی که خبرنگاران بی‌بی‌سی با جزولی تماس گرفتند، او اعتراف کرد که مجری این کمپین بوده است. او با مرکز جنگالا کار می‌کند، سازمانی که توسط معاون رئیس جمهور



اندونزی، یوسف کالا، ایجاد شده است. کالا این سازمان را در سال ۲۰۱۴ برای تبلیغ انتخاب مجدد خود و حمایت از دولت رئیس‌جمهور جوکو ویدودو ایجاد کرده بود.

آنچه این تحقیق نشان می‌دهد این است که شناسایی کمپین‌های اطلاعاتی و نسبت دادن آن‌ها به افراد و گروه‌های مسئول الزاما به تکنیک‌ها یا ابزارهای پیچیده نیاز ندارد؛ اما هم به صبر و هم به مقدار مشخصی شانس نیاز است. این تحقیق به منابع منبع‌باز مانند سوابق Whois، جستجوی معکوس عکس، حساب‌های کاربری در رسانه‌های اجتماعی و تجزیه و تحلیل کدهای منبع وب‌سایت‌ها متکی بود. این واقعیت که این کمپین در چندین پلتفرم در حال اجرا بود در کنار حساب‌های کاربری شبکه‌های اجتماعی و پروفایل لینکدین متعلق به کارمندان اینسایت آی‌دی به ما کمک کرد سرنخ‌های کوچک متعدد را در کنار هم بچینیم و موفق به دیدن تصویر کلی‌تر شویم.

اگر یک درس کلیدی برای آموختن از این مثال وجود داشته باشد آن درس این است که چگونه می‌توانید با استفاده از جزئیات یا سرنخ‌های موجود در یک پلتفرم برای چرخش به پلتفرم‌های دیگر استفاده کنید.

تهیه‌کنندگان:

ویراستار: کرگ سیلورمن

ویراستار همکار: کلر واردل

ویرایشگر: مریل پرلمن

با مشارکت: بن کالینز، بن نیمو، بنجامین استریک، برندی زادرازنی، شارلوت گدار، کلر واردل، کرگ سیلورمن، دونی اُسالیوان، الیز توماس، فریدا ویس، گابریل لیم، جما باگایاو-مندوزا، هانا گای، هنک ون‌اس، جین لیتوین‌نکو، جوآن دانه‌ون، یوهانا وایلد، سم گرگوری، سرژو لوتسکی، سایمون فاکنر، ورنیس تانتوکو

مدیر تولید: آرنه گرال

این کتاب توسط مرکز روزنامه‌نگاری اروپا منتشر شده است و انتشار آن به لطف کمک مالی از سوی خیریه کرگ نیومارک امکان‌پذیر شده است.

این راهنما، توسط فکت‌نامه و حمایت اصل۱۹ به فارسی برگردانده شده است.