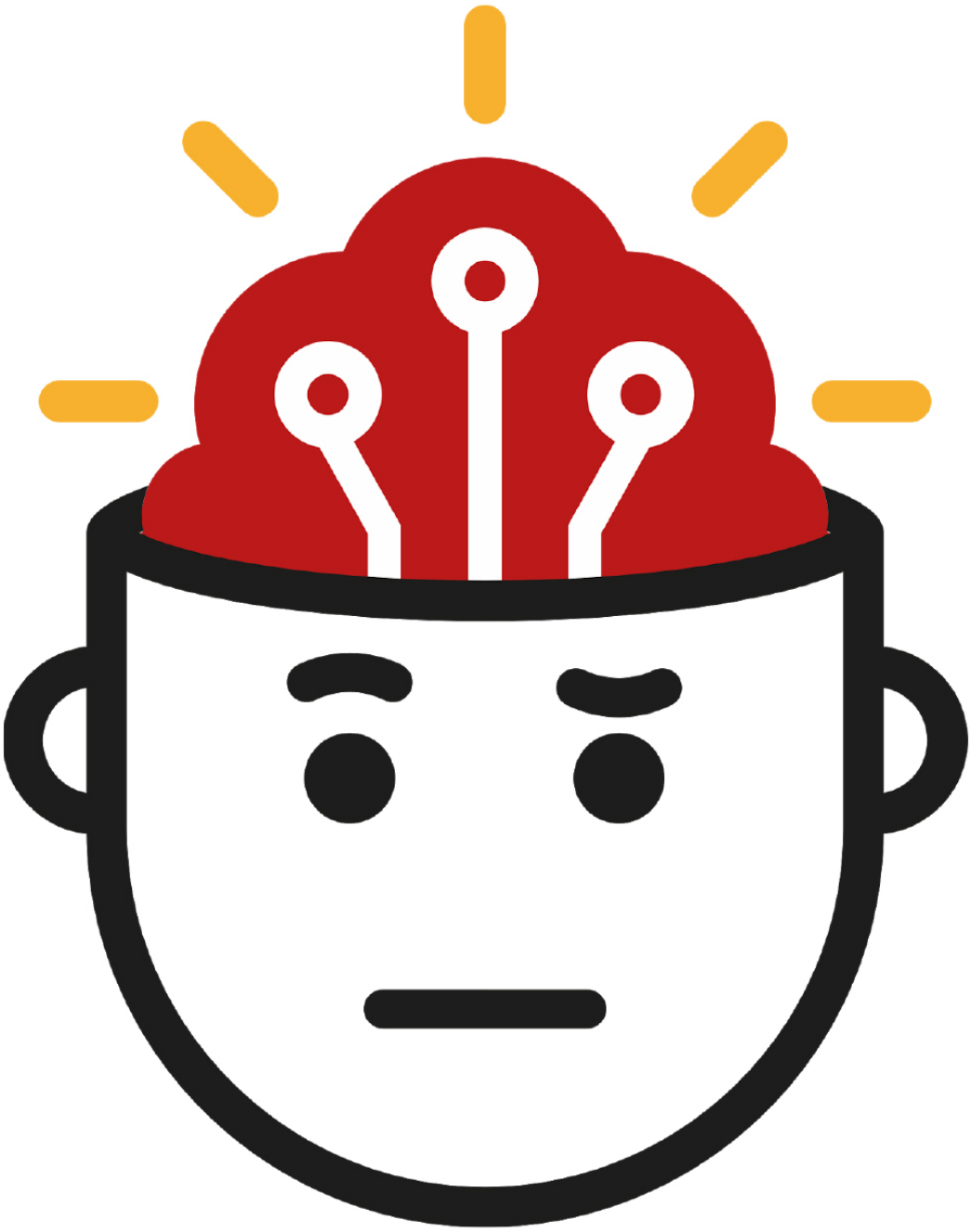
Прирачник за верификација

За дезинформации и медиумски манипулации

Ултимативен водич за истражување на платформите и корисничките сметки на интернет за откривање на неавтентични активности и манипулирани содржини



Уредник: Крег Силверман

Изданието на Прирачникот за верификација за дезинформации и медиумски манипулации го подготви
Центарот за развој на медиуми од Скопје

ЦЕНТАР за РАЗВОЈ на МЕДИУМИ

Овој проект е поддржан од Амбасадата на САД. Мислењата, откритијата и заклучоците или препораките изнесени овде се на имплементаторите/ авторите, и не ги одразуваат оние на Владата на САД

Превод: Дејан Георгиевски
Технички уредник: Љубен Димановски

Февруари 2024

ПОГЛАВЈА

4..... Истражување на дезинформациите и медиумските манипулации

8..... Ера на информативен неред

14..... Животниот циклус на медиумските манипулации

19..... 1. Истражување на корисничките сметки на социјалните медиуми

35..... 1а. Студија на случај: Како истражувањето на група кориснички сметки на Фејсбук откри оркестриран потфат за ширење пропаганда во Филипините

41..... 1б. Студија на случај: Како докажавме дека најголемата Фејсбук-страница посветена на Black Lives Matter („Црните животи се важни“) е лажна

46..... 2. Откривање на нултиот пациент

55..... 3. Препознавање на ботови, киборзи и неавтентични активности

65..... 3а. Студија на случај: Пронаоѓање докази за автоматизирани активности на Твитер за време на протестите во Хонгконг

75..... 4. Мониторинг за откривање лажни информации во периоди на ударни вести

86..... 5. Верификација и проверка на слики и илустрации

96..... 6. Како да размислуваме за „длабоките фалсификати“ и новите технологии за манипулација

103..... 7. Следење и известување од затворени групи и апликации за испраќање и примање пораки

108..... 7а. Студија на случај: Болсонаро во болницата

111..... 8. Истражување на интернет страници

123..... 9. Анализа на рекламите на социјалните мрежи

136..... 10. Следење на движењето на актери преку повеќе платформи

143..... 11. Анализа на мрежи и атрибуција

152..... 11а. Студија на случај: Атрибуција во случајот „Бескрајна мајска мушичка“ (Endless Mayfly)

158..... 11b. Студија на случај: Истражување на информативна операција во Западна Папуа

161..... За авторите

Истражување на дезинформациите и медиумските манипулации

Автор: Крег Силверман

Крег Силверман *(Craig Silverman) е медиумски уредник на BuzzFeed News, каде го предводи глобалниот тим за покривање на платформите, дезинформациите во онлајн сферата и медиумските манипулации. Претходно ги приреди „Прирачникот за верификација" и „Прирачникот за верификација за истражувачко новинарство", и е автор на „Лаги, проклети лаги и вирални содржини: Како информативните веб-страници шират (и раскринкуваат) онлајн гласини, непотврдени тврдења и мисинформации" (Lies, Damn Lies, and Viral Content: How News Websites Spread (and Debunk) Online Rumors, Unverified Claims and Misinformation).*

Во декември 2019 година, корисникот на Твитер @NickCiarelli (Ник Сијарели) сподели видео за кое тврдеше дека прикажува танц што поддржувачите на претседателската кампања на Мајкл Блумберг (Michael Bloomberg) го прифатиле како официјален танц на кампањата. Видливиот недостиг на ентузијазам кај танчерите и „лабавата" кореографија прикажани на видеото веднаш придонесоа тоа да собере многу ре-твитови и допаѓања, првенствено од луѓе што уживаа да се потсмеваат со него. Видеото било прегледано повеќе од 5 милиони пати на Твитер .

Според биографијата на Сијарели на профилот на Твитер, тој бил ангажиран во кампањата на Блумберг како стажист, а неговите последователни твитови вклучувале и докази за тој ангажман, на пример, слика од е-маил порака од лице што наводно работело за кампањата на Блумберг што содржела одобрување на буџет за изработка на видеото.

Брзо претражување на неговото име на Гугл покажа дека се работи за комичар кој и претходно произведувал и поставувал комични видеа. Што со е-маил пораката од вработениот кај Блумберг? Испратена е од Бред Еванс (Brad Evans), чест соработник на Сијарели во подготовка на комични материјали. Сè што требаше да направиме за да ја пронајдеме таа информација беше едноставно пребарување на Гугл.

Сепак, во првите минути и часови по објавувањето, некои луѓе поверуваа дека таквото чудно видео и официјално е дел од продукцијата на Блумберг.

Меги Хаберман (Maggie Haberman), позната политичка новинарка на Њујорк Тајмс, објави твит дека новинарите што известувале за претходните кампањи на Блумберг на изборите за градоначалник имале добри причини да не го отфрлат видеото на прво гледање:

Знаењето има многу форми, а во новото дигитално опкружувања, новинарите треба да внимаваат да не зависат премногу од кој било извор на информации - дури и ако се работи за претходно позитивно искуство од прва рака.

Очигледно, некои новинари кои го познаваат Блумберг и неговиот стил на водење кампања сметале дека видеото би можело да биде автентично. Истовремено, новинарите што не знаеле ништо за Блумберг и избрале својата оценка за видеото да ја засноваат на тоа кој е изворот, можеле да ги добијат точните одговори веднаш - во овој случај, едноставно да го „изгуглаат“ името на лицето што го споделило.

Поентата не е дека известувањето за Блумберг е лошо искуство. Поентата е дека во секој момент можеме да бидеме заведени на погрешен пат од нешто за што мислиме дека добро го знаеме. А во некои случаи, нашето претходно знаење и искуство можат да играат и негативна улога. Можеме да бидеме заведени од различни дигитални сигнали како што се ретвитови и прегледи, или од обиди за нивна манипулација.

Како што покажува видеото за Блумберг, не мора да се вложи многу труд да се создадат заведувачки сигнали како што се биографијата на корисничката сметка на Твитер или снимката од е-маил порака што ја потврдува содржината и изнесените тврдења. Тоа, од своја страна, помага содржината да стане вирална. Што повеќе ретвитови и допаѓања ќе собере, полесно ќе им биде на таквите сигнали да убедат некого дека видеото може да биде и вистинско.

Се разбира, има и далеку поподли примери од овој. За разлика од Сијарели, луѓето што стојат зад различни информативни операции и кампањи за дезинформирање ретко ја откриваат измамата. Сепак, оваа студија на случај покажува колку збунувачко и фрустрирачко е за сите, вклучувајќи ги и новинарите, да се снаоѓаат во информативно опкружување полно со сигнали за квалитет и доверба со кои лесно може да се манипулира.

Довербата е во основата на секое општество. Таа ги формира и подмачкува сите трансакции и е клучна за човечките врски и односи. Од друга страна, во нашето дигитално опкружување е опасно да се работи на ниво на автоматска доверба.

Ако автоматски верувате дека сметките на Твитер што ретвитуваат едно видео го амплифицираат органски, лесно ќе бидете прелажани. Ако верувате дека сите рецензии за некој производ се дадени од вистински потрошувачи, ќе ги фрлите парите во ветер. Ако верувате дека секоја статија во вашиот преглед на вести (news feed) претставува непристрасен збир на она што навистина треба да го видите, на крај ќе бидете лошо информирани.

Иако е важно сите да ја препознаат таа реалност, за новинарите тоа е од клучно значење. Ние сме цел на координирани, добро финансирани кампањи што целат да го окупираат нашето внимание, со измама да не натераат да амплифицираме некои пораки, и да станеме подложни на волјата на државата и на други центри на моќ.

Добрата вест е што сето тоа создава можност - и императив - за истражување.

Овој прирачник произлегува од знаењето и искуствата на врвни новинари и истражувачи за да обезбеди упатства за начинот на водење на истраги на операциите за дигитални медиумски манипулации, дезинформирање и информирање.

Работиме во комплексен информативен еко-систем што брзо се менува. Тоа бара подеднакво еволутивен пристап заснован на преиспитување на нашите претпоставки, следење и предвидување на потезите на противниците и примена на најдобрите техники на истражување со отворени извори и на техниките за традиционалното известување. Слабостите на овој дигитален свет придвижуван од податоци бара од новинарите да ги преиспитаат и истражат сите негови аспекти и да ги применат своите вештини за да и помогнат на јавноста да стигне до точни и веродостојни информации. Исто така, од новинарите бара да размислуваат на кој начин, не сакајќи, можеби ги помагаме злонамерните актери и кампањи направени со цел да не искористат, и брзаме да посочиме со прст кон државните актери дури и во случаи кога доказите не поддржуваат таков заклучок.

Целта на овој прирачник е да ги опремиме новинарите со потребните вештини и техники за да можат успешно и одговорно да ја извршуваат таа задача. Прирачникот нуди и основни сознанија за теоријата, контекстот и мисловниот склоп што им овозможува на новинарите квалитетно да работат и да ја информираат јавноста, да ги изнесат на светлото на денот злонамерните актери, и да помогнат во подобрувањето на нашето информативно опкружување. Сепак, првата работа што треба да ја разбереме е дека од практичното знаење и алатките ќе нема никаква полза ако на задачата не и пристапиме со правилен начин на гледање на работите.

Тоа значи разбирање дека во дигиталното опкружување може да се игра и манипулира со сè, како и разбирање на широкиот дијапазон на луѓе и субјекти што имаат корист од манипулациите. Убавината на дигиталното опкружување е што често, иако не секогаш, постои трага од податоци, односи, врски и други дигитални „ронки“ што можат да се следат. Поголемиот дел од тие траги се јавно достапни, само треба да знаете каде и како да барате.

Истражувањето во дигиталната средина значи дека ништо не треба да прифатиме така како што изгледа на прв поглед. Тоа значи разбирање дека она што изгледа дека може да се квантифицира и е придвижувано од податоци - допаѓања, споделувања, ретвитови, сообраќај, рецензии на производи, кликнувања на реклами - може лесно да се манипулира и често е манипулирано. Значи препознавање дека новинарите се во фокусот на информативни операции за медиумски манипулации, и како цел на нападите, и како клучен канал за ширење на погрешните информации и дезинформациите. Конечно, значи дека треба да се опремите себе и вашите колеги со светоглед, техники и алатки потребни за да се обезбедите дека ќе нудите веродостојни и точни информации - и нема да засилувате лажни, манипулирани содржини или кампањи за „тролување“.

Во сржта на вистинскиот начин на размислување се наоѓа парадоксот на дигиталното истражување: Ако од почеток пристапиме со недоверба, можеме да се зафатиме со работата што ќе ни открие што треба а што не треба да веруваме. И тоа ќе ни овозможи да понудиме производ на кој заедниците на кои им служиме ќе сакаат и ќе можат да му веруваат.

Освен тоа, постојат неколку темелни идеи што се повторуваат и нагласуваат во одделните поглавја и студии на случаи наведени во прирачников:

- Размислувајте како вашите противници. Секоја нова функционалност на некоја платформа или дигитална услуга може да биде експлоатирана на еден или на друг начин. Од клучно значење е да се поставите во позиција на некој што сака да го манипулира опкружувањето поради идеолошки, политички, финансиски или други причини.
- Кога ги разгледувате дигиталните содржини и пораки, треба да размислите која била мотивацијата за нивно создавање и ширење. Исто така, треба да бидете упатени во најновите техники што ги користат злонамерните актери, експертите за дигитален маркетинг и други лица и субјекти што заработуваат од пронаоѓање нови начини на привлекување внимание во дигиталното опкружување.
- Фокусирајте се на актерите, содржините, однесување и мрежите. Целта е да ги анализираме актерите, содржините и однесувањето и да документираме дали тие можеби функционираат едногласно, како мрежа. Преку меѓусебна споредба и ставање во контраст на овие четири работи, можете да почнете да разбирате што точно гледате. Како што ќе видите во неколку поглавја и студии на случаи, во основата на пристапот е да се почне со една содржинска единица или со еден субјект, на пример, интернет страница и таа да служи како централна точка во идентификацијата на поширока мрежа преку однесувањето на актерите и други врски. Тоа може да вклучува испитување на протокот на содржини и актери преку различни платформи, а повремено и на различни јазици.
- Следете и собирајте. Најдобар начин за идентификување на медиумските манипулации и дезинформации е постојано да ги барате. Во основата се работи за постојан мониторинг и следење на движењето на познатите актери, темите и заедниците од интерес. Чувајте ги вашите наоди во организирана форма, на сметководствени табели, папки со снимки од прикази на екранот, или со користење на платени алатки како што е Hunchly.
- Внимавајте при атрибуцијата. Понекогаш е невозможно точно да се утврди кој стои зад одредена корисничка сметка, содржина или поширока информативна операција. Една причина за тоа е можноста актери со различна мотивација да се однесуваат на сличен начин, и да произведуваат или поддржуваат ист вид на содржина. Дури и платформите - иако имаат многу подобар пристап до податоците и повеќе ресурси на располагање - прават грешки во атрибуцијата и наведувањето на авторството. Најуспешните и најубедливите докази вообичаено комбинираат дигитални докази со информации добиени од внатрешни извори - идеална комбинација од традиционална и онлајн истражувачка работа. Тоа станува дури и потешко знаејќи дека државните и други актери развиваат и наоѓаат нови начини за да ги сокријат своите траги. Атрибуцијата е тешка; секоја грешка може да ги поткопа сиот труд и внимание што ве довеле до заклучокот.

Конечно, неколку зборови за двата прирачници што му претходеа на ова издание. Овој труд претставува надградба на темелите поставени во првото издание на „Прирачникот за верификација“ и на „Прирачникот за верификација за истражувачко новинарство“. Двата прирачници ги нудат основните вештини за следење на социјалните медиуми, верификација на слики, видеа и кориснички налози на социјалните медиуми, како и за користење на пребарувачите за идентификација на луѓе, компании и други субјекти.

Повеќето поглавја и студии на случаи во овој прирачник се пишувани со претпоставка дека читателите ги имаат основните знаења наведени во претходно објавените изданија, особено во првиот прирачник. Ако имате потешкотии во следењето на ова издание, препорачувам да почнете со првиот прирачник.

А сега, да се зафатиме со работа.

Ера на информативен неред

Автор: Клер Вордл

Клер Вордл (Claire Wardle) *го предводи одделот за стратегиски правци и истражување во „Прв нацрт" (First Draft), глобална непрофитна организација што им дава поддршка на новинарите, членовите на академската заедница и технолозите во наоѓањето одговори на предизвиците поврзани со довербата и вистината во дигиталната ера. Работела како соработник на Шоренстеин центарот за медиуми, политика и јавни политики на Кенеди школата на Харвард (Fellow at the Shorenstein Center for Media, Politics and Public Policy, Harvard's Kennedy School), Директор за истражувања на Тоу центарот за дигитално новинарство на Школата за пост-дипломски студии по новинарство на Универзитетот Колумбија (Tow Center for Digital Jounalism, Columbia University's Graduate School of Journalism), и раководител за социјални медиуми во УНХР, Агенцијата за бегалци на ОН.*

Сите знаеме дека лагите, гласините и пропагандата не се нови концепти. Луѓето отсекогаш имале способност да мамат и знаеме за повеќе славни историски примери на времиња во кои фабрификувани содржини беа користени за заведување на јавноста, дестабилизација на влади или да им се помогне на берзанските индекси да раснат. Она што денес е ново е лесноТијата со која секој може да создаде убедливи лажни и заведувачки содржини, како и брзината со која таквите содржини ќе го обиколат светот.

Отсекогаш сме биле свесни дека мамењето е комплексна работа. Еден конфекциски број не им се фаќа на сите. На пример, добронамерна лага кажана за да се зачува мирот за време на семејна кавга не е исто како и заведувачка изјава дадена од политичар кој се обидува да придобие што повеќе гласачи. Пропагандна кампања спонзорирана од државата не е иста со некоја теорија на заговор за слетувањето на месечината.

За несреќа, во последниве неколку години, сè што може да влезе во категориите опишани овде добиваше етикета „лажни вести", едноставен термин што се стекна со глобална популарност, често и без потреба да се преведува кога се користи во други јазици.

Велам за несреќа, бидејќи тој термин е трагично несоодветен за опишување на сложената ситуација што ја гледаме околу нас. Повеќето содржини што се заведувачки на еден или на друг начин не се ни обидуваат да се маскираат како вести. Се работи за „мимови", видеа, слики или координирани активности на Твитер, Јутјуб, Фејсбук или Инстаграм. И повеќето од нив не се лажни; тие се заведувачки или, што е почест случај, вистински но користени надвор од својот контекст.

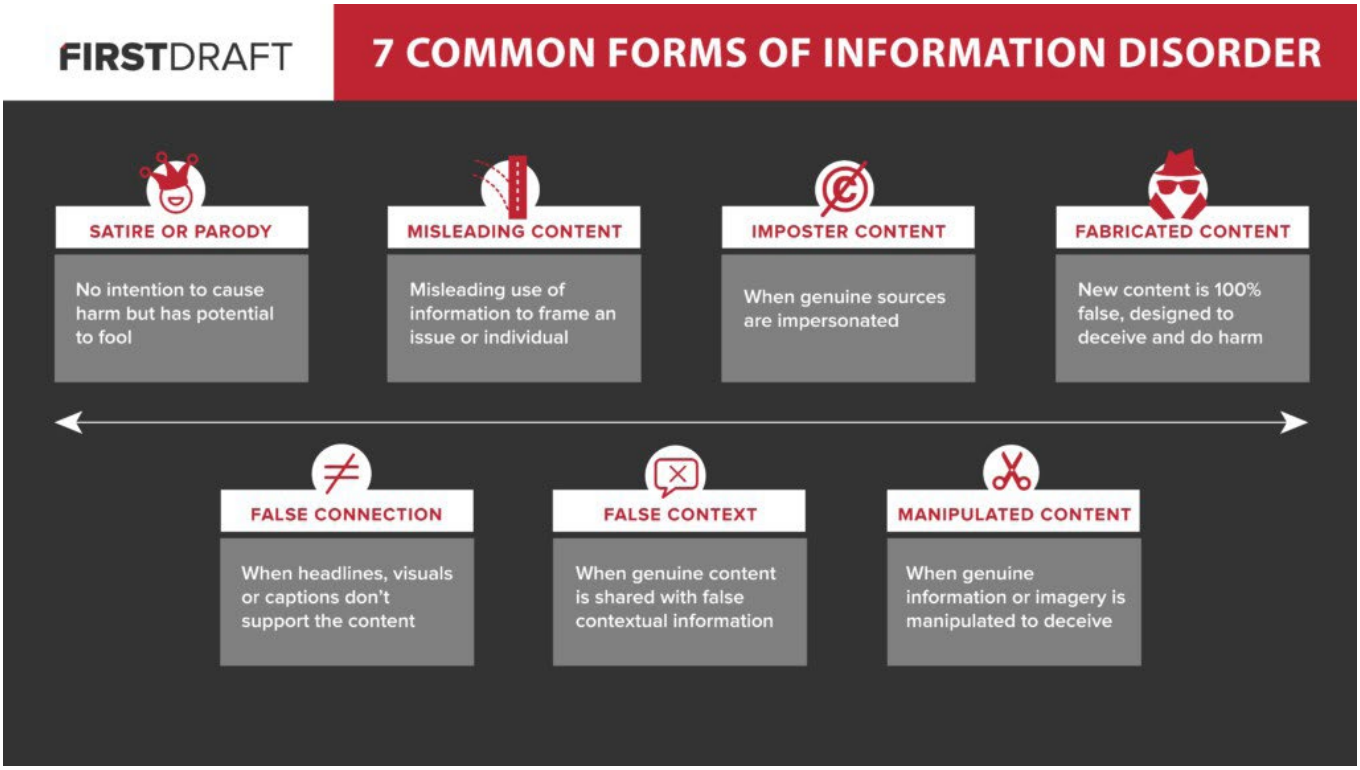
Токму дезинформациите што во себе имаат барем 'ркулец на вистина постигнуваат најголем ефект: ќе земете нешто што е вистинито и погрешно ќе го означите, или ќе споделите нешто што всушност е три години старо како ново.

Најголем проблем веројатно е тоа што терминот „лажни вести" стана оружје што политичари и нивни поддржувачи го користат за напад врз професионалните информативни медиуми ширум светот.

Мојата лична фрустрација со таа фраза ме доведе то тоа да ја смислам фразата „информативен неред", заедно со ко-авторот Хосеин Деракшан (Hossein Derakhshan). Во 2017 година напишавме извештај со наслов „Информативен неред" и во него ги истраживме предизвиците што ги носи постоечката терминологија на таа тема. Во ова поглавје, ќе понудам објаснување за некои од клучните дефиниции аспекти за разбирањето на оваа тема и нивното критичко разгледување.

7 видови на информативен неред

Во 2017 година ја понудив следната типологија за да ги потцртам различните видови на информативен неред што постојат.



„7 ЧЕСТИ ФОРМИ НА ИНФОРМАТИВЕН НЕРЕД“

САТИРА ИЛИ ПАРОДИЈА – нема намера да се предизвика штета, но има потенцијал да излаже или заведе
ЗАВЕДУВАЧКА СОДРЖИНА – заведувачка употреба на информации за врамување на некое прашање или личност
НАТРАПНИЧКА СОДРЖИНА – кога се имитираат постоечки извори
ФАБРИКУВАНА СОДРЖИНА – Новата содржина е сто отсто лажна, наменета да измами и да нанесе штета
ЛАЖНА ВРСКА – кога насловите, илустрациите и легендите под нив не соодветствуваат на содржината
ЛАЖЕН КОНТЕКСТ – Кога вистинска содржина се споделува со лажни информации за контекстот
МАНИПУЛИРАНА СОДРЖИНА – кога се манипулира со вистински информации или слики со цел да се измами

Сатира/Пародија

Разбирливо, многу луѓе не се согласуваат со мојата одлука во типологијата да ја вклучам и сатирата, а секако и самата имав дилеми околу тоа прашање. За жал, агентите на дезинформациите намерно ги означуваат содржините како сатира за да обезбедат дека нема да бидат подложени на „проверка на фактите“, и во обид да се амнестираат за каква било штета што нивната содржина би можела да ја предизвика. Во информативниот екосистем од кој се отстранети контекстот и знаците, или менталните кратенки (хевристика), постои поголема веројатност сатиричните содржини да го збунат или залажат читателот. Обичен Американец може да знае дека „Онион“ (The Onion, кромид) е сатиричен вебсајт, но дали знаевте дека, според Википедија (Wikipedia), во светот постојат 57 сатирични информативни вебсајтови? Ако не сте запознаени дека веб-страницата што ви прелетува пред очи на Фејсбук е сатирична, лесно можете да бидете излажани.

Фејсбук неодамна одлучи дека нема да врши проверка на факти за сатирата, но оние што работат во оваа област добро знаат дека етикетата сатира намерно се користи како фасада. Всушност, во август 2019 година, американската организација за разоткривање на лажни информации „Сноупс“ (Snopes) објави статија наведувајќи ги причините поради кои тие спроведуваат проверка на факти и за сатирични содржини. Содржини што се прикажани како сатира ќе ја избегнат проверката на фактите и често, како што минува времето, изворниот контекст се губи: луѓето ги споделуваат и проследуваат тие содржини без да разберат дека содржината е сатирична, верувајќи дека е вистинита.

Лажна врска

Сè работи за старата добра „мамка за кликови“ (click-bait): техника на изнесување тврдења за содржината преку сензационалистички наслов, за подоцна да откриеме дека насловот скоро и да нема врска со соодветната статија или содржина. Иако за информативните медиуми е лесно да размислуваат за дезинформацијата како за проблем што го предизвикуваат злонамерни актери, јас тврдам дека треба да се знае дека лошите практики во новинарството носат дополнителни предизвици во информативниот неред.

Заведувачки содржини

Ова е нешто што отсекогаш било проблем во новинарството и во политиката. Било да се работи за избор на одделен сегмент од некоја изјава, креирање на статистички податоци што поддржуваат одредено тврдење без водење сметка како е создаден сетот на податоци, или „кроење“ на некоја фотографија за некој настан да се врами на посакуваниот начин, овие видови на заведувачки практики секако не се нови.

Лажен контекст

Ова е категоријата во која влегува најголемото количество на содржини: се јавува речиси секогаш кога оригинални слики одново се споделуваат како нови. Често се случува за време на настани што претставуваат ударни вести, кога повторно се објавуваат стари слики и илустрации, но се случува и кога стари новински статии одново се споделуваат како нови, ако насловот сè уште потенцијално може да се поврзе со современите настани.

Натрапничка содржина

Овде се работи за случаи кога логото на добро-познат бренд или нечие име се користи заедно со лажна содржина. Оваа тактика е од стратешка природа затоа што се потпира на важноста на хеуристиката. Еден од најмоќните начини на кои судиме за содржината е дали е создадена од организација или од лице во кои веќе имаме доверба. Значи, со преземање на логото на веродостојна новинска организација и негово приложување кон некоја фотографија или видео, автоматски ја зголемувате можноста дека луѓето ќе ѝ веруваат на содржината без да ја проверат.

Манипулирана содржина

Се работи за случаи кога оригинална содржина е обработувана или менувана на некаков начин. Пример за тоа е видеото со Ненси Пелоси (Nancy Pelosi) од мај 2019 година. Претседателката на Претставничкиот дом на САД беше снимена додека држи говор. Само неколку часа подоцна, се појави видео од нејзиниот говор на кој таа звучеше како да е пијана. Видеото било успорено за да изгледа како таа да ги заплеткува зборовите. Се работи за потентна тактика, затоа што е заснована на оригинална, вистинска снимка. Ако луѓето знаат дека таа го одржала говорот, на таа сцена, уште повеќе ќе му веруваат на она што го гледаат.

Фабрикувана содржина

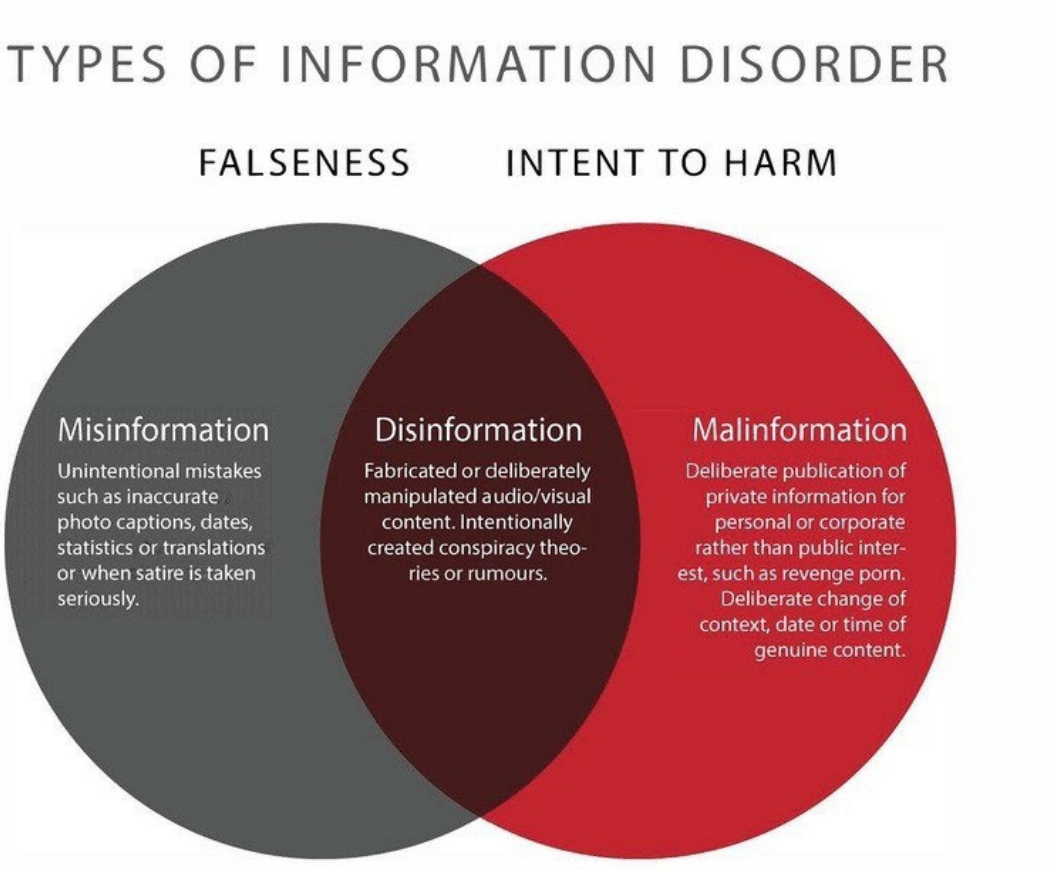
Во оваа категорија влегува содржината што е 100 отсто фабрикувана. Може да се однесува на подготовка на целосно нова, лажна корисничка сметка на социјалните медиуми преку која ќе се шират нови содржини. Во оваа категорија влегуваат и тн. „длабоки фалсификати“ (deepfake) каде со помош на вештачка интелигенција се изработува видео или аудио документ во кој некое лице говори или прави нешто што никогаш не се случило.

Разбирање на намерата и мотивацијата

Наведените типови се корисни за објаснување на комплексната природа на загаденото информативно опкружување, но не се занимава со прашањето на намерите. А тоа е клучното прашање за разбирање на тој феномен.

За да дадеме одговор на тоа прашање, со Деракшан нацртавме Венов дијаграм за да ги објасниме разликите помеѓу мисинформациите, дезинформациите и третиот термин што го сковавме, злонамерните информации (malinformation). Мисинформациите и дезинформациите се примери за лажна содржина. Разликата е во тоа што дезинформацијата е создадена и споделувана од луѓе кои сакаат да предизвикаат штета, без оглед дали се работи за финансиска, политичка, физичка штета или штета на нечија репутација. Мисинформациите исто така се лажни, но луѓето што ги споделуваат содржините не знаат дека се лажни. Тоа често се случува со настани што претставуваат ударни и вонредни вести, кога луѓето споделуваат гласини или стари фотографии без да се свесни дека тие не се поврзани со тековниот настан.

Кај злонамерната информација се работи за вистинска и вистинита информација, но луѓето што ја споделуваат се обидуваат да предизвикаат штета. Пример за тоа е објавувањето на е-маил пораките на Хилари Клинтон (Hillary Clinton) за време на Претседателските избори во САД во 2016 година. Друг пример е споделувањето на тн. „одмаздничка порнографија“.



ВИДОВИ НА ИНФОРМАТИВЕН НЕРЕД
СТЕПЕН НА ЛАЖНОСТ / НАМЕРА ДА СЕ НАНЕСЕ ШТЕТА

Мисинформации – Ненамерни грешки како што се погрешни легенди на фотографии, погрешени датуми, статистички податоци или погрешен превод, или кога сатирата се сфаќа сериозно.
Дезинформации – Фабрикувани или намерно манипулирани аудио/визуелни содржини. Намерно креирани теории на заговор или гласини.
Злонамерни информации – Намерно објавување на приватни информации од личен или корпоративен, но не и од јавен интерес, како што е одмаздничката порнографија. Намерно менување на контекстот, датумот или точното време во оригиналната, вистинска содржина.

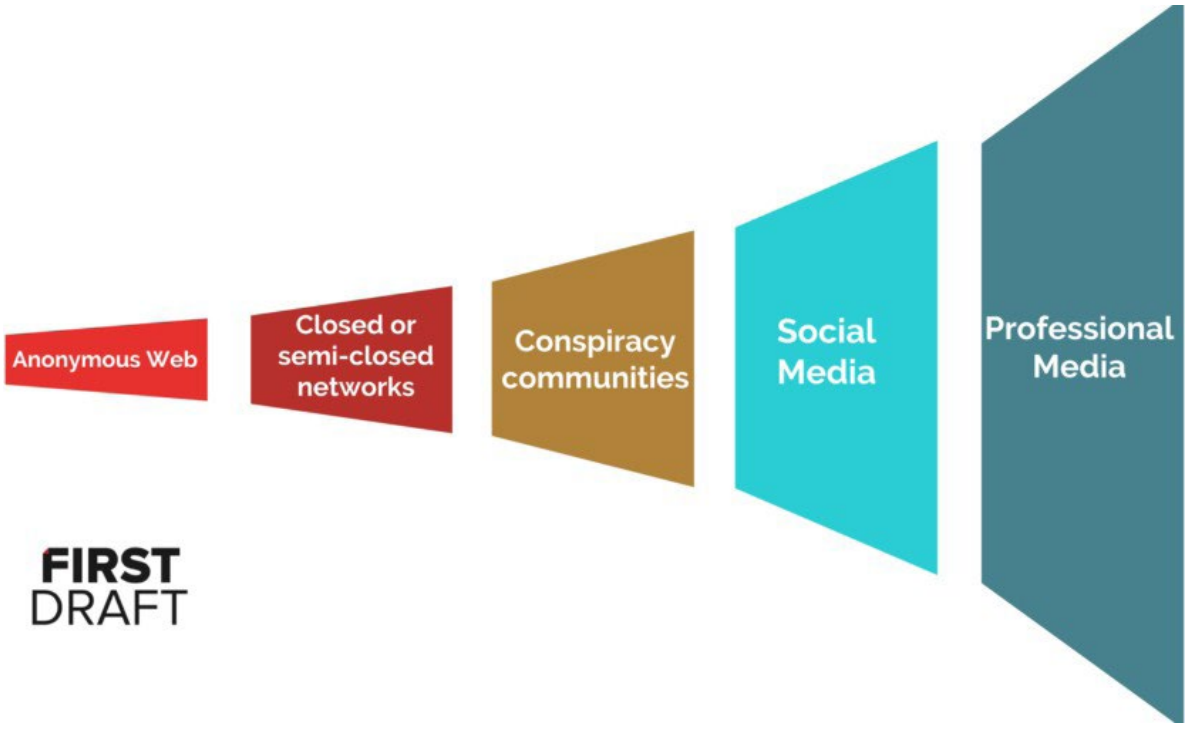
Терминологијата е значајна затоа што разбирањето на намерата е дел од разбирањето на одредена информација. Постојат три главни мотиви за создавање на лажни и заведувачки содржини. Првиот мотив е политички, било да се работи за надворешна или за внатрешна политика. Можеби се работи за обид на странска влада за мешање во изборите во друга земја.

Можеби се работи за внатрешна политика при што нечија изборна кампања применува „валкани“ тактики за оцрнување на противниците. Вториот мотив е од финансиска природа.
Постои можност за заработка од продажба на рекламен простор на вашата веб-страница. Ако имате сензационалистичка, лажна статија со хиперболичен наслов, сè додека успевате да ги привлечете луѓето да кликнат на вашата УРЛ адреса, можете да заработите. Луѓе на двете страни на политичкиот спектар отворено кажуваат дека создавале фабрикувани „новински“ сајтови за да привлечат кликови, а со тоа и приходи. Конечно, во игра се и одредени општествени и психолошки фактори. Некои луѓе едноставно се мотивирани од желбата да предизвикуваат проблеми за да проверат дали можат да поминат неказнето; да проверат дали можат да ги излажат новинарите, да создадат настан на Фесјбук што ќе ги извади луѓето на улица да протестираат, да ги вознемируваат или да им се закануваат на жените. Други споделуваат мисинформации при што единствена причина е желбата да застапуваат одреден идентитет. Такви се, на пример, оние што велат „Не ми е грижа дали ова е вистина или не, само сакам да им покажам на пријателите на Фејсбук колку го мразам (внесете го името на кандидатот што го мразат)“.

Труба за амплификација

За вистински да го разбереме овој поширок екосистем, треба да согледаме на кој начин сето тоа е поврзано меѓу себе. Пречесто се случува некој да види некаде накаква заведувачка или лажна содржина и да верува дека е создадена таму каде што ја видел. За несреќа, оние што имаат најголем успех на полето на дезинформациите знаат како најдобро да ја искористат фрагментираната природа на екосистемот.

Запомнете дека ако гласините, заговорите и лажните содржини не беа споделувани, немаше да предизвикаат никаква штета. Токму споделувањето ја причинува најголемата штета. Поради тоа ја создадов следната слика што ја нарекувам Труба за засилување, како начин да опишам како агентите на дезинформирањето координирано ја движат информацијата низ екосистемот.



Анонимен веб
Затворени или полу-затворени мрежи
Заедници собрани околу заговори
Социјални медиуми
Професионални медиуми

Пречесто содржината е поставена на простори како што се „4Чен“ (4Chan) или „Дискорд“ (Discord, апликација за комуникација што ја користат играчите на видео-игри). Тие простори овозможуваат анонимно користење и поставување на содржини без каква било задршка. Често таквите простори се користат за споделување на специфични упатства за координиран настап, на пример, „ќе се обидеме да направиме овој хаштаг да стане тренд“, или „користете го овој „мим“ за да одговорите на денешните настани на Фејсбук“.

Координацијата потоа често преминува на големите за размена на пораки на Твитер (Twitter DM - direct message, апликација за размена на пораки - Твитер ДМ) или на „Вотсап“ (WhatsApp), каде јазлите поврзани во една мрежа ја прошируваат содржината до поголеми групи луѓе. Потоа може да премине во заедниците на сајтови како што се „Габ“ (Gab), „Редит“ (Reddit) или „Јутјуб“ (YouTube). Оттаму, содржината често ќе биде споделувана и на по-мејнстрим сајтовите како што се Фејсбук, Инстаграм или Твитер.

Понатаму ќе биде преземена од професионалните медиуми кои или, затоа што не го знаат потеклото на таа содржина, решиле да ја искористат во известувањето без доволно проверки, или решиле да ја раскринкаат таа содржина. Во секој случај, агентите на дезинформирањето на тоа гледаат како на успех. Лошите наслови што пренесуваат гласина или заведувачко тврдење, или статиите за раскринкување каде лажната содржина е вградена во приказната, одат на рака на изворниот план: да се поттикне амплификацијата, на гласината да и се дадат крилја.

„Фирст драфт“ го користи концептот за „точка на прекршување“. За новинарите, прераното известување за лажните информации на една гласина и обезбедува дополнителен и потенцијално штетен ветер во грбот. Ако за неа се известува предоцна, тоа значи дека фатила корен и веќе не може да се направи многу во борбата против неа. Определувањето на таа точка на прекршување е голем предизвик. Моментот во кој настапува се разликува од тема до тема, од една локација или платформа до друга.

Заклучок

Важно е каков јазик користиме. Се работи за комплексен феномен и зборовите што ги користиме можат да направат клучна разлика. Веќе постојат академски истражувања што покажуваат дека публиката сè почесто ја изедначува фразата „лажни вести“ со лоши новинарски практики во професионалните медиуми.

Опишувањето на сè живо како дезинформација, и во случаи кога можеби содржината не е лажна, или е несвесно споделувана од луѓе кои не мислат дека е лажна, се другите клучни елементи на разбирањето што точно се случува.

Живееме во ера на информативен неред. Тој неред пред новинарите, истражувачите и професионалците во областа на информирањето поставува нови предизвици. Да се извести или не? Како да го срочиме насловот? Како ефективно да ги раскринкаме видеата или сликите? Како ќе знаеме кога да се зафатиме со раскринкување? Како ја мериме и определуваме точката на прекршување? Се работи за нови предизвици за оние што работат во информативното опкружување. Работата не е лесна.

Животниот циклус на медиумските манипулации

Автор: Џоан Донован

Др. Џоан Донован (Joan Donovan) *е директорка за истражувања во Шоренстајн центарот за медиуми, политика и јавни политики на Кенеди школата на Харвард (Shorenstein Center for Media, Politics and Public Policy, Harvard›s Kennedy School)*

Во време во кое еден грст моќни глобални технолошки платформи ги пореметија традиционалните средства за информирање на општеството, кампањите за медиумски манипулации и дезинформирање поставуваат предизвици пред сите политички и општествени институции. Измамите и фабрикациите ги шири мешана група од политички оперативци, брендови, општествени движења и неврзани „тролови“ кои развиле и усовршиле нови техники за влијание врз јавната дискусија, ширејќи хаос на локално, национално и глобално ниво. Постои широко распространета согласност дека медиумските манипулации и дезинформациите се значајни проблеми со кои се соочува општеството. Но дефинирањето, откривањето, документирањето и раскринкувањето на дезинформациите и медиумските манипулации останува тешко, особено затоа што нападите покриваат повеќе професионални сектори како што се новинарството, правото и технологијата. Оттаму, разбирањето на медиумските манипулации како активност што следи одредени шеми и урнеци на однесување е клучниот прв чекор во работата на нивно истражување, разоткривање и ублажување на последиците.

Дефинирање на медиумските манипулации и дезинформации

За да ја дефинираме медиумската манипулација, најпрво тој термин треба да го расчлениме на неговите составни делови. Во своето најопшто значење, медиум е артифакт за комуникација. Примери за медиуми се текст, слики, аудио или видео записи на материјални или на дигитални медиуми. Кога ги проучуваме медиумите, секоја останка може да се искористи како запис за некој настан. Клучно е дека медиумите се создадени од индивидуи со цел да комуницираат нешто. Медиумите пренесуваат некакво значење помеѓу лицата, а толкувањето на значењето секогаш зависи од постоечките односи и е ситуирано во контекстот на дистрибуцијата.

Тврдењето дека медиумите се манипулирани оди подалеку од едноставното тврдење дека медиумите се направени од индивидуи за да пренесат некакво целно значење. Речникот Мериам-Вебстер (Merriam-Webster) ја дефинира манипулацијата како „промена на нешто, со вештина или со нечесни средства, за да послужи на нечија цел“. Иако понекогаш тешко може да се знае со која цел е создаден некој артифакт, истражувачите можат да утврдат кој е кој, што е што, каде е каде и како е како во комуникацијата на тој артифакт, што ќе им помогне во утврдувањето дали се користени манипулативни тактики како дел од дистрибутивниот процес. Манипулативните тактики можат да вклучуваат прикривање на нечиј идентитет или на изворот на артифактот, уредување за да се прикрие или промени значењето или контекстот на артифактот, и мамење на алгоритимите со користење на средства за вештачка координација како што се ботовите или алатките за спамирање.

Во тој контекст, дезинформацијата е под-жанр на медиумската манипулација и се однесува на намерното создавање и дистрибуција на лажни информации за остварување на политички цели. Технолозите, експертите, припадниците на академската заедница, новинарите и носителите на политики мораат да се согласат за тоа што сè влегува во засебната категорија на дезинформации затоа што борбата против дезинформациите бара соработка на сите тие групи.

Од наша страна, истражувачкиот тим за Технологии и општествени промени (Technology and Social Change - TaSC) на Шоренстајн центарот на Кенедиевата школа на Универзитетот Харвард го користи пристапот на студија на случај за да го мапира животниот циклус на кампањите за медиумски манипулации. Таквиот методолошки приод бара анализа на редот, обемот и опфатот на кампањите за манипулација преку следење на медиумски артифакти низ просторот и времето, извлекувајќи повеќекратни односи за да воспостави ред во замрсениот неред. Како дел од нашата работа, развивме преглед на животниот циклус на кампања за медиумски манипулации што им користи на новинарите во обидите да ги идентификуваат, следат и разоткријат манипулациите и дезинформациите.

Животен циклус на една кампања за медиумски манипулации

1.Планирање на кампања за манипулација
2.Расејување на кампањата преку социјалните платформи и на интернет
3.Одговор на индустријата, активистите, политичарите и новинарите
4.Промени во информативниот екосистем
5.Прилагодување на манипулаторите на новото опкружување

Животниот циклус има пет точки на дејствување во кои тактиките на медиумските манипулатори можат да бидат документирани со користење на квалитативни и квантитативни методи. Имајте на ум дека за најголем број кампањи за манипулација „откривањето“ не оди нужно по тој редослед. Наместо тоа, кога истражувате, барајте која било од тие точки на дејствување и потоа следете ја кампањата наназад или нанапред низ животниот циклус.

Студија на случај: „Дувни во свирката"

Да ги разгледаме активностите на социјалните медиуми поврзани со жалбата на еден „свиркач" за активностите на претседателот Доналд Трамп (Donald Trump) во врска со Украина, за да видиме како се одвива една кампања за медиумска манипулација и како етичките дејства на новинарите и платформите во раниот стадиум на животниот циклус можат да помогнат да се спречат обидите за манипулација.

Планирање и расејување (Фази 1 и 2) - Во медиумскиот екосистем на теориите на заговори, идентитетот на „свиркачот" е веќе познат и неговото име циркулира на блогови, на Твитер, Фејсбук, на видоа на јутјуб и на форумите за дискусија.
Треба да се знае дека имињата можат да ги заменат клучните зборови и хаштаговите што функционираат како дискретни податочни точки што можат да бидат пребарувани. Постоеше оркестриран напор да се прошири и разгласи наводното име и фотографијата на лицето. Сепак, изгледа дека името остана затворено во медиумската онлајн ехо-комора на десничарски и конспираторски кориснички сметки и субјекти. Дури и со таков координиран напор на инфлуенсерите што се занимаваат со теории на заговор да го пренесат името на наводниот свиркач во мејнстримот, не успеаја да се пробијат надвор од сопствените филтрирачки меури. Зошто се случи тоа?

Одговори од новинари, активисти итн. (Фаза 3) – Сосема спротивно, левичарските и центристичките медиуми не го објавија името на наводниот свиркач и не ги амплифицираа тврдењата дека неговиот идентитет е откриен. Мејнстрим медиумите останаа воздржани и не обрнаа внимание на циркулирањето на името на тоа лице во екосистемот на социјалните медиуми, и покрај тоа што се работи за приказна интересна како вест за новинарите што покриваат технологија и политика. Оние што известуваа за таа тема често посочуваа дека чинот на циркулирање на името и идентитетот е обид за манипулирање на дискусијата за поплаките на свиркачот и избегнуваа натамошно ширење на неговиот идентитет. Тоа во голема мерка се должи на новинарската етика и посебната обврска за новинарите да ја штитат анонимноста на изворите која ги покрива и свиркачите.

Промени во информативниот екосистем (Фаза 4) - Иако новинарите од мејнстрим медиумите не го спомнуваа, наводното име на свиркачот, „Ерик Сијарамела" (Eric Ciaramella), е уникатен клучен збор. Тоа значи дека луѓето што го пребаруваа тој клучен збор можеа да извлечат многу разновидни содржини со корен во ставовите обоени од различни теории на заговор. Покрај одбивањето на етичките новинари да пишуваат за приказна што би можела да привлече големо внимание и сообраќај, компаниите што управуваат со платформите почнаа со активно модерирање на содржините што го користеа наводното име на свиркачот како клучен збор. Јутјуб и Фејсбук ги отстранија содржините што го содржеа неговото име, а Твитер спречи името да стане „тренд". Пребарувачот на Гугл, од друга страна, дозволуваше пребарување на името и прикажуваше илјадници линкови до блогови посветени на теории на заговор.

Прилагодување на манипулаторите (Фаза 5) - Манипулаторите беа бесни на таквите обиди да се спречи ширењето на погрешните информации и ја променија тактиката. Наместо да ги „туркаат“ содржините со наводното име на свиркачот, манипулаторите почнаа да пуштаат во оптек фотографии на друг бел маж (со очила и брада) кој наликуваше на сликата што, заедно со името, претходно беше пуштена во циркулација. Новите слики одеа рака под рака со конспиративен наратив за „длабоката држава“ (deep state) според кој свиркачот е пријател на естаблишментот на Демократската партија и бил партиски мотивиран.
Сепак, се работеше за фотографија на Александар Сорос (Alexander Soros), син на милијардерот, инвеститор и филантроп Џорџ Сорос (George Soros), кој е честа цел на теориите на заговор.

Откако тоа не успеа да привлече медиумско внимание, корисничката сметка на Твитер на претседателот Трамп, @RealDonaldTrump, до своите 68 милиони следбеници ретвитуваше статија во која беше наведено наводното име на свиркачот, со потенцирање дека „Свиркачот на ЦИА не е вистински свиркач!“ Оригиналниот твит дојде од сметката @TrumpWarRoom, официјалната верификувана сметка на неговата изборна кампања. Следеше поплава од медиумско известување, во кое се вклучија и многу мејнстрим медиуми, при што сите се трудеа да го отстранат или да го покријат наводното име на свиркачот. Многу луѓе побараа, преку социјалните медиуми, свиркачот да се појави како сведок на сослушувањето за отповик во Сенатот на кое, покрај други важни потенцијални сведоци, беше спомнато и неговото име, отворајќи можност другите да наидат на него пребарувајќи ги другите имиња на интернет. Така започна нов циклус на медиумска манипулација.

Бројот на пребарувања на името на свиркачот растат а на блоговите се множат заговорите за неговите лични и професионални мотиви да информира за активностите на Трамп. Новинарските извештаи за твитовите се движат од дискусија за прашањето на заплашување на сведоците, наведувајќи дека дејства како прикажаните можат да ги одвратат идните свиркачи, до изливи на злорадосно љубопитство преку известување на гласините и озборувањата за мотивите на Трамп да го открие идентитетот на наводниот свиркач.

За поздравување е тоа што некои медиумски организации се обидуваат да ги повикуваат елитите на одговорност, но таа задача е невозможна без компаниите што управуваат со платформите да го разгледаат прашањето како нивните производи се претворија во корисни политички алатки за медиумски манипулации и ширење на дезинформации.

Документирање на животниот циклус

Медиумските манипулатори се обидоа да „прескокнуваат скалила“ преку расејување на име и фотографии на социјалните медиуми за евентуално да ги предизвикаат големите, легитимни медиуми да ја амплифицираат таа приказна, а платформите да дозволат приказната да влезе во тренд и да може лесно да се пронајде на интернет. Но одлуките и дејствата на платформите и новинарите значеа дека обидот да се истурка наводниот идентитет на свиркачот во свеста на мејнстримот беше претежно неуспешен, сè додека со прашањето не се зафати личност за која постои интерес во јавноста.

Додека многу медиумски организации се стремат да ги почитуваат етичките правила, социјалните медиуми станаа оружје на оние што веќе имаат моќ да ја диктираат агендата на медиумите и да промовираат опасни заговори.

Сепак, општо земено, оваа студија на случај претставува значајно подобрување во споредба со претходните обиди да се сопре ширењето на дезинформации, каде новинарите ги засилуваа кампањите за дезинформирање во обидите да ги раскринкаат, а компаниите што управуваат со платформите не чувствуваа никаква обврска на публиката да и обезбедат точни информации. Таквото престројување ветува, но сè уште недостига одговорноста на елитите. За новинарите, како и за академските истражувачи, влогот во откривањето, документирањето и раскринкувањето на кампањите за медиумски манипулации е голем. Во хипер-партизираната сегашност, секој обид да се посочи на некоја кампања за дезинформирање може да ви навлече на грб орди од тролови и многу несакано внимание. Справувањето со содржината и контекстот на дезинформацијата бара од сите нас форензички строг приод во документирањето на почетокот, текот и промените и крајот на кампањите. Исто така, бара да прифатиме дека секој претпоставен крај на една кампања може со голема веројатност да означува и нов почеток.

1. Истражување на корисничките сметки на социјалните медиуми

Автор: Бренди Задрозни

Бренди Задрозни (Brandy_Zadrozny) *е истражувачки новинар во ЕнБиСи Њуз (NBS News), и главно ги покрива темите како што се погрешно информирање, дезинформации и екстремизам на интернет.*

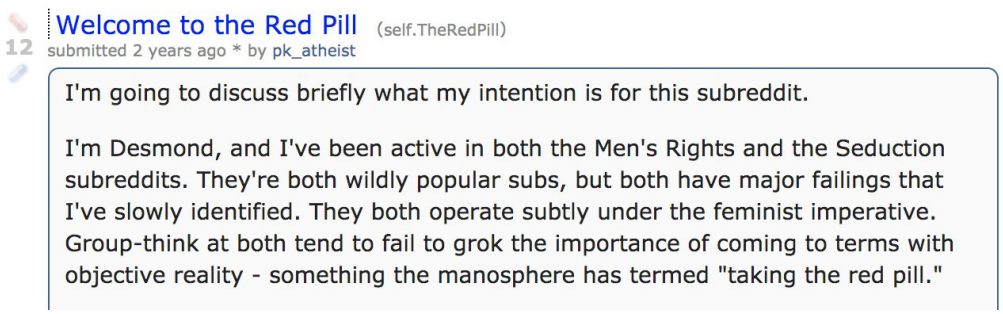
Скоро сите приказни за кои известувам вклучуваат и детективска работа на социјалните мрежи. Од истражување кој стои зад некој профил до ударни вести и подолги истражувања, платформите на социјалните медиуми нудат одлични можности да дознаете нешто за животот на некое лице - семејството, пријателите, кариерата, политичките ставови и врски - како и увид во тајните мисли и скриените онлајн-идентитети.

Ова е неверојатно време да се биде новинар; луѓето се повеќе ги живеат животите во онлајн просторот а алатките за откривање и пребарување на социјалните профили се сеприсутни. Истовремено, и обичниот свет и злонамерните актери се сè повешти во прикривањето на своите траги. Во меѓувреме, платформите за социјални медиуми како што е Фејсбук реагираа на лошиот публицитет што го добија поради нарушувањата на приватноста и ширењето на штетни идеологии преку нивните платформи со затворање на алатките на кои новинарите и истражувачите се потпираа во откривањето на приказните и идентификацијата на инволвираните актери.

Во следното поглавје, ќе прикажам неколку основни приоди за истражување на корисничките сметки на социјалните медиуми. Прикажаните алатки се оние што во моментов ги користам, но на Фејсбук нема да му треба многу време да ги укине или да ги замени со подобри. Известувачите што најдобро ја работат оваа работа си имаат сопствени процеси и уреди да стигнат до целта, но, реално, како и кај сите видови новинарство, опсесивниот приод и (виртуелното) „кинење чевли“ даваат најдобри резултати. Бидете подготвени да прочитате илјадници твитови, да кликате на линкови до крајот на листата на резултати на Гугл, и да нурнете во дувлото на социјалните медиуми ако сакате да ги соберете ситните биографски ронки што ќе ви помогнат да одговорите на прашањето „Кој е ова?“

Кориснички имиња

Понекогаш сè што имаме на почетокот е корисничко име, и тоа е во ред, затоа што тоа е точката од која најчесто тргаме во истражувањето. Таков беше и случајот со тогаш новоизбраниот член на претставничкиот дом на Њу Хемпшир од Републиканската партија, кој изгради еден од најпопуларните и најомразените заедници на мажи на Редит (Reddit). Истражувањето за демаскирање на архитектот на „Црвеното апче“ (The Red Pill) на Редит, која сега е заедница во карантин, почна со корисничкото име „pk_atheist“.



Некои луѓе се приврзани за своите кориснички имиња, ги користат со минимални варијации на повеќе платформи или за електронска пошта. Оние што повеќе се ориентирани кон безбедноста, како што е претставникот од Њу Хемпшир, ги менуваат и креираат нови кориснички имиња за секој нов потфат.

[–] **pk_atheist** [S] 2 points 3 years ago

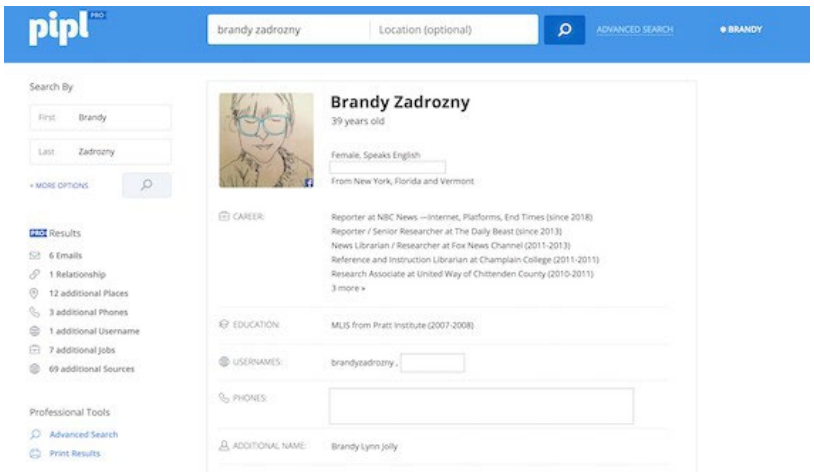
I don't think we can grow if we ever go private. It goes without saying, you should invest in a decent throwaway that cannot be traced back to you.

permalink embed parent

Во секој случај, постојат неколку интернет страници во кои треба да го внесете корисничкото име што го истражувате.

Прво го внесувам корисничкото име во Гугл. Луѓето - особено помладите што ги избегнуваат големите социјални платформи - знаат да остават траги на многу неочекувани места, вклучувајќи ги секциите за коментари, рецензии или на форумите, што можат да ве одведат до повеќе информации и до други кориснички сметки.

Покрај пребарувањето на Гугл, користете и специјализирани комерцијални сервиси. Нивното користење чини пари и можеби ќе можете да им пристапите, можеби не, во зависност од буџетот со кој располага редакцијата. Во повеќето продавници може да се купи „Нексис“ (Nexis), одличен сервис за пребарување низ јавни и судски архиви, но, за жал, слаб на полето на електронската пошта/кориснички имиња. Исто така, корисен е за истражување на индивидуални лица само во САД. „Пипл“ (Pipl) и „Скоупнау“ (Skopenow) се некои од најдобрите алатки што ми се познати што служат за вкрстување на информации од „реалниот свет“, како што се телефонски броеви и катастарски канцеларии, со онлајн записи како што се електронска пошта и кориснички имиња. Двата сервиси функционираат глобално. Овие платени пребарувачи често обезбедуваат записи за корисниците на телефони како и податоци за сопственоста над недвижнини, но можат и да идентификуваат профили на Фејсбук или Линкдин (LinkedIn) дури и за веќе затворени кориснички сметки. Тие, исто така, поврзуваат кориснички сметки што дури и корисниците заборавиле дека ги имале, како што се стари блогови, па дури и листи на желби од „Амазон“ (Amazon) - вистинско закопано богатство ако сакате да дознаете што некој чита, купува или посакува. На тие сервиси се добиваат и многу лажни позитивни резултати, така што преферирам истражувањето да го почнам со резултатите што сум ги добила од нив и да продолжам со други средства за верификација.



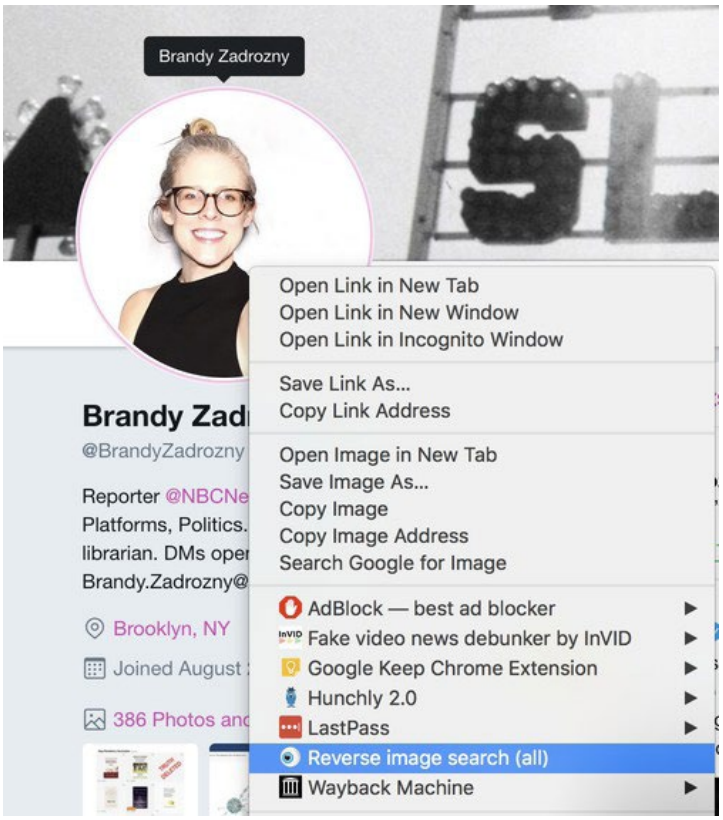
Кога ќе пронајдам корисничко име или е-маил адреса за кои сметам дека можеби му припаѓаат на субјектот на истрагата, ги проверувам на онлајн алатки како што се „na-mechk“ или „namecheckr“, кои пребаруваат достапност на кориснички имиња преку повеќе платформи. Тие алатки се наменети за специјалистите за маркетинг да можат полесно да видат дали корисничкото име што сакаат да го регистрираат е слободно на повеќе платформи. Корисни се и ако сакате да проверите дали некаде постои корисничкото име што е предмет на истражувањето. Очигледно, тоа што некое корисничко име е регистрирано на повеќе платформи не мора да значи дека сите кориснички сметки му припаѓаат на исто лице. Сепак, тоа е одлична почетна точка за разгледување преку повеќе платформи.

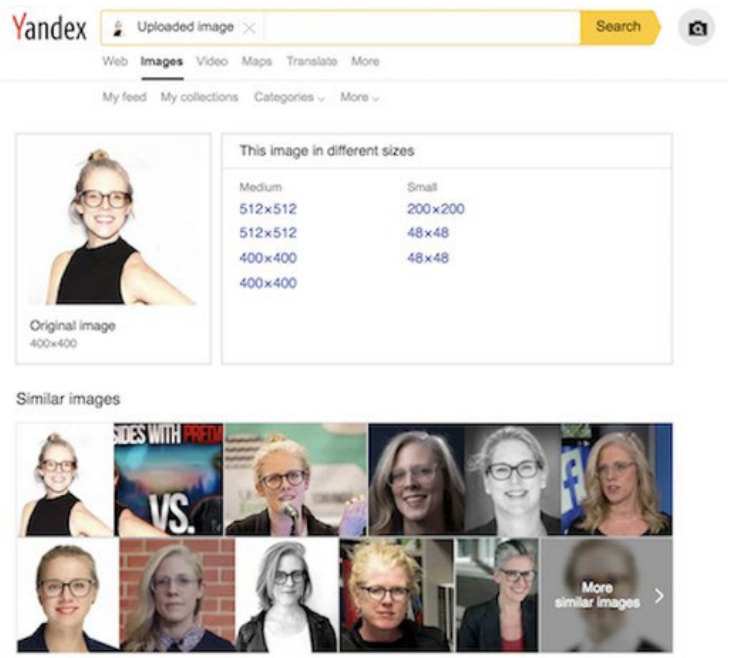
За дополнителни проверки на кориснички имиња, тука се и haveibeenpwned.com и Dehashed.com, алатки што пребаруваат кориснички информации во протечени податоци и можат брзо да потврдат некоја е-маил адреса и да сугерираат нови траги.

Фотографии

Корисничкото име не секогаш е доволно да се продолжи понатаму, а ништо не е толку убедливо како прикажана фотографија. Профилните фотографии се друг начин за верификација на идентитетот на едно лице на повеќе кориснички сметки.

Реверзибилното пребарување на слики (reverse image search) на Гугл е добра опција, но често други пребарувачи - особено рускиот „Јандекс“ (Yandex) - можат да испорачаат подобри резултати. Јас ја користам екстензијата „Ревај“ (Reveye) на „Хром“ (Chrome), што овозможува, со десен клик на сликата, да се побара идентична слика на повеќе платформи, вклучувајќи ги Гугл, Бинг (Bing), Јандекс и Тинај (Tineye). Екстензијата „Пребарување со слика“ (Search by Image) содржи и одлична функција за „зафаќање“ што овозможува пребарување на слика што се содржи во друга слика.

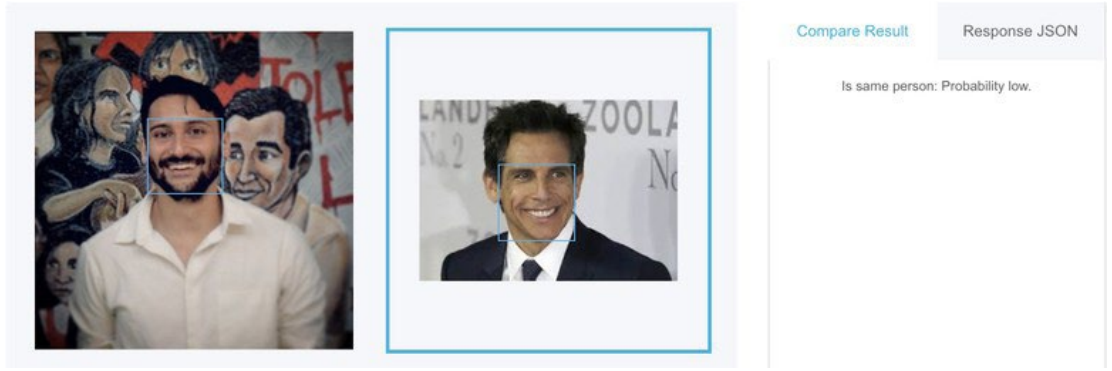




Сè разбира, при реверзибилното пребарување на слики постојат и проблеми. Спомнатите пребарувачи се лоши за пребарување на слики на Твитер, и скоро сосема бескорисни ако барате резултати на страници како Инстаграм или Фејсбук.

Она што најчесто го гледам пред себе се слики од различни луѓе. Не можам ни да избројам колку пати сум се фатила самата себе како „зјапам“ во мониторот, прашувајќи ги колегите „Ова истото лице ли е?“

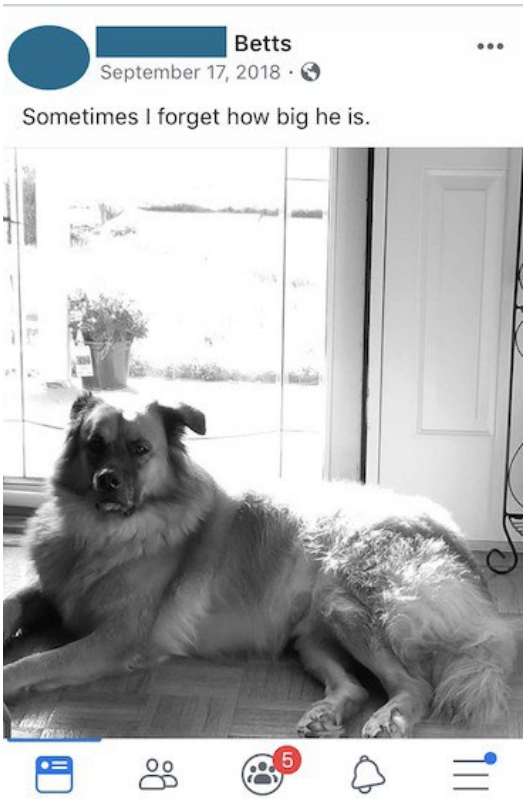
Едноставно, не им верувам на сопствените очи. Препознавањето на исти карактеристики како што се бемки, брада, или специфична физиономија на повеќе фотографии е од голема помош; од неодамна, исто така преферирам да ги проверувам фотографиите со алатки за препознавање на лица како што е „Фејс++“ (Face++), што овозможува поставување на две фотографии една до друга и потоа ви дава информација за веројатноста на нив да е снимено истото лице. Во посочените примери, алатката успеа позитивно да ме идентификува на фотографии снимени секои десет години. Таа, исто така, го идентификуваше мојот колега Бен на профилните фотографии на Твитер и Фејсбук, забележувајќи правилно дека тој не е актерот Бен Стилер (Ben Stiller).

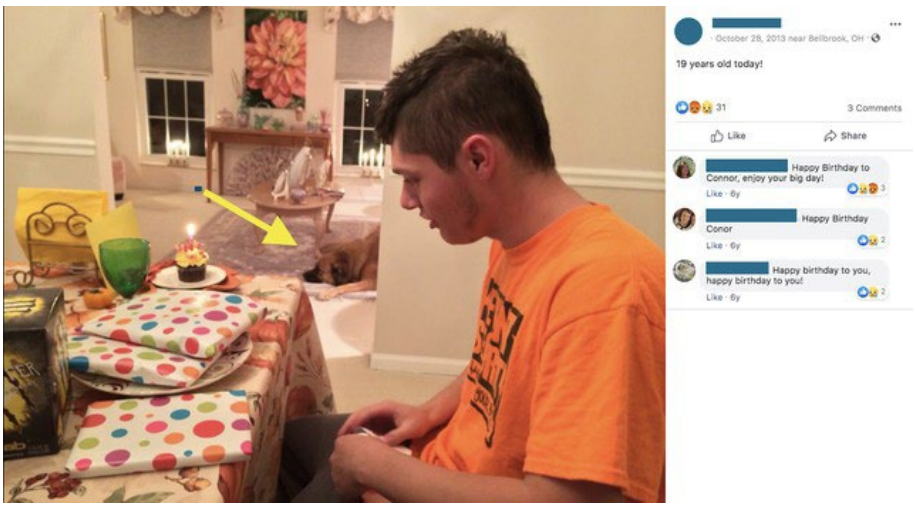


Ако сте во потера по тролови или „скамери“ (scammers - измамници), можеби ќе откриете дека се потрудиле да ја замаглат профилната фотографија, или можеби користат лажни фотографии. Ако при обработката на фотографијата ја превртиме по нагорна оска во обратна ориентација, тоа може да го следи процесот на обработка што тие го примениле во обратна насока.

Профилните фотографии не се единствени што можат да послужат како патокази. Иако луѓето стануваат посвесни и позагрижени за својата приватност и за приватноста на нивните семејства, сè уште се склони да споделуваат фотографии од она со што се гордеат. Сум идентификувала луѓе преку поврзување на фотографии од автомобили, куќи или домашни миленици. Од таа гледна точка, фотографиите стануваат средство за поврзување на корисничките сметки и луѓето што стојат зад нив, што ви овозможува да исплетете мрежа околу вашата цел. Тоа е основна постапка при истражувањето на кориснички сметки на социјалните медиуми.

На пример, се обидувавме да ги потврдиме корисничките сметки на социјалните мрежи на еден маж што пукаше и смртно застрела девет лица пред еден бар во Дејтон, Охајо. Неговата корисничка сметка на Твитер понуди одредени показатели за неговата политичка идеологија, но неговиот „прекар“ (handle) @iamthespookster, беше уникатен и не потсетуваше со ништо на вистинското име што беше објавено од властите. Фактот дека една од жртвите е негов брат, трансродов маж чие име не беше наведено во јавните архиви и кој претходно не го открил јавно својот родов идентитет, дополнително го усложни процесот на идентификација на клучните фигури во случајот. Но на неговиот профил и на профилите на членовите на неговото семејство беа објавени слики од пес, домашен миленик чија слика служеше како банер (banner) на необјавената корисничка сметка на неговиот трансродов брат.





Песот не беше единствениот корисен детал на горната слика. Таа слика ја добивме од таткото на стрелецот од Охајо и ни помогна да ги верификуваме неговите лични кориснички сметки и сметките на членовите на неговото семејство.

Ако имате корисничка сметка на Фејсбук или на Твитер, веројатно можам да ви кажам кога ви е роденден, дури и ако тој податок не сте го споделиле јавно на вашиот профил или не сте објавиле пост за него. Ако знаеме дека датумот на раѓање често е една од првите информации за идентификација што полицијата ги дава кога се случуваат вонредни вести, еден сигурен начин за верификација на корисничка сметка на социјалните медиуми е да се „скролува“ до соодветниот ден и месец на сметката што ја проверуваме и да побараме дали има роденденски честитки. Дури и ако нивните страни се празни, често родителите (како родителите на Конор Бетс (Connor Betts) на горната слика ќе напишат нешто за роденденте на нивните деца.

Истото важи и за Твитер. Конечно, има ли некој што не сака роденденi?

На Твитер е дури и полесно да се пронајде пост што ќе помогне во идентификацијата, затоа што неговата алатка за пребарување е помеѓу најдобрите од алатките што ги нудат социјалните платформи. Иако скоро никогаш, или многу ретко, кажувам кога ми е роденден, успеав да пронајдам роденденски „твит“ од еден љубезен колега кој ја „откри мојата тајна“.

Родендените се само еден пример. Венчавки, погреби, годишни одмори, годишнини, дипломирања - скоро сите големи денови што ни ги обележуваат животите се прославуваат на социјалните медиуми. Сите тие нудат отворена врата за пребарување и истражување на некоја корисничка сметка.

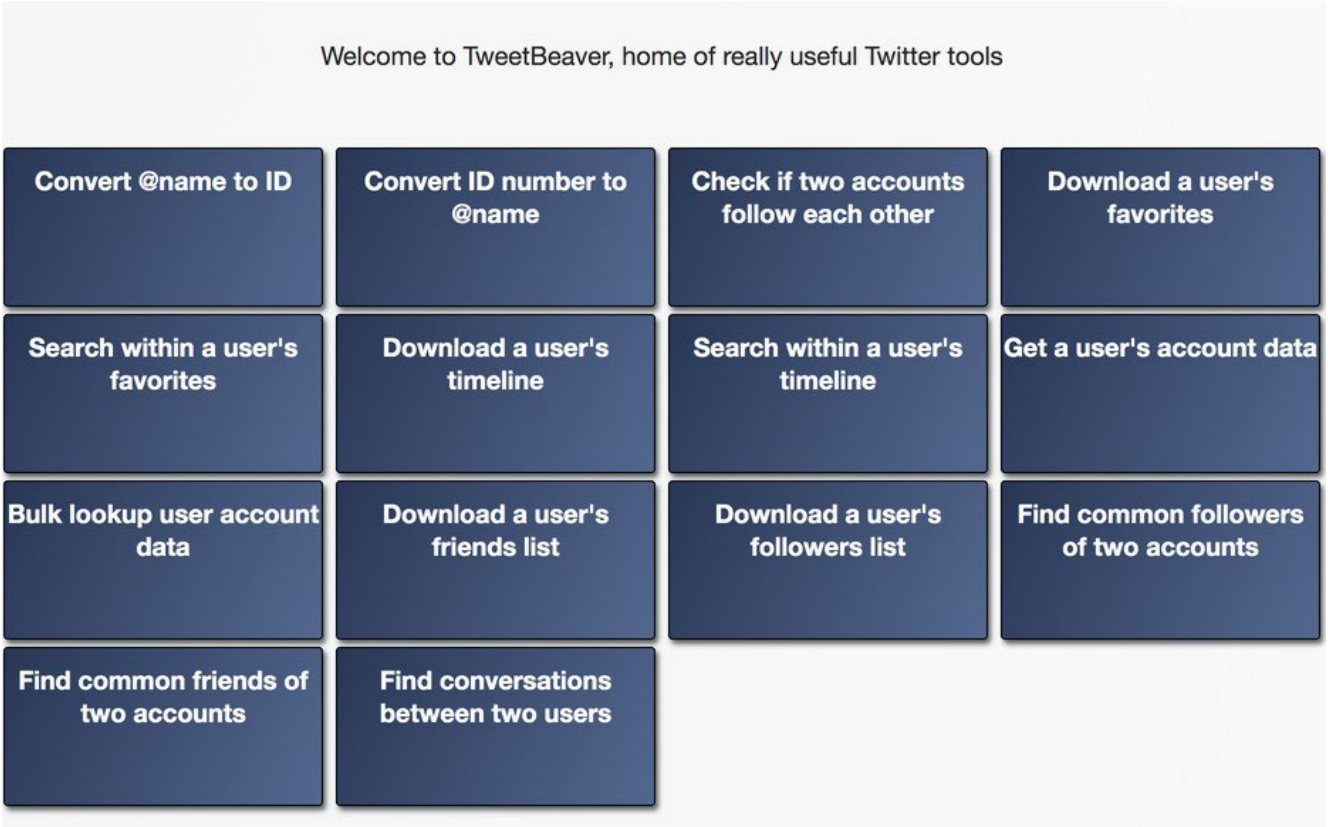
Можете да пребарувате со клучни зборови, или со други филтри на алатките за пребарување на Фејсбук. Веќе не одат толку далеку како во времето пред платформата да се сврти кон поголема приватност, но сè уште постојат. Една од моите омилени алатки е whopostedwhat.com.

Врски

Можете да оцените некого според тоа со кого се дружи на социјалните медиуми. Можеме да дознаеме многу за нечиј живот и склоности преку преглед на луѓето со кои комуницира на интернет.

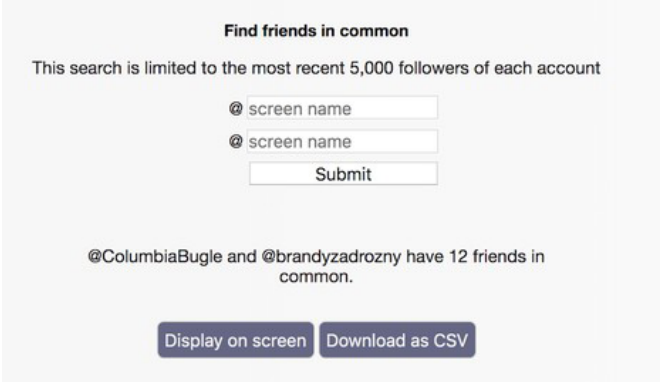
Кога прв пат се приклучив на Твитер, ги натерав и сопругот и мојата најдобра пријателка да се приклучат, само за да можат да ме следат. Размислувам за тоа кога пребарувам кориснички налози што ми требаат за работата. Ниту платформите не сакаат да сте сами, па кога прв пат ќе отворите корисничка сметка, се вклучува еден алгоритам. Под влијание на листата на контакти на вашиот телефон, дали се појавувате на листите за контакти на веќе постоечки кориснички налози, локацијата на која се наоѓате и други фактори, платформата ќе ви сугерира кориснички сметки што можете да ги следите.

Поради тоа, секогаш е полезно да ги прегледате најраните следбеници и пријатели на некоја корисничка сметка. ТвитБивер (TweetBeaver) е добра алатка за истражување на врските помеѓу големи кориснички сметки и за снимање, на пример, на хронолошки прегледи или фаворитите наведени на помалите кориснички сметки. За поголеми сетови на податоци, се потпирам на услугите на еден девелопер што има пристап до АПИ (API, application programming interface).

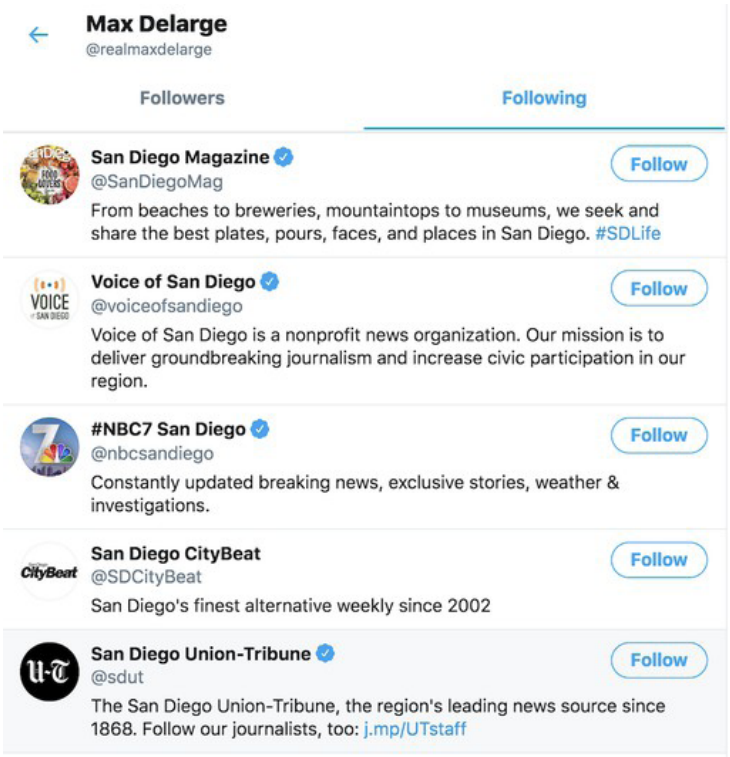


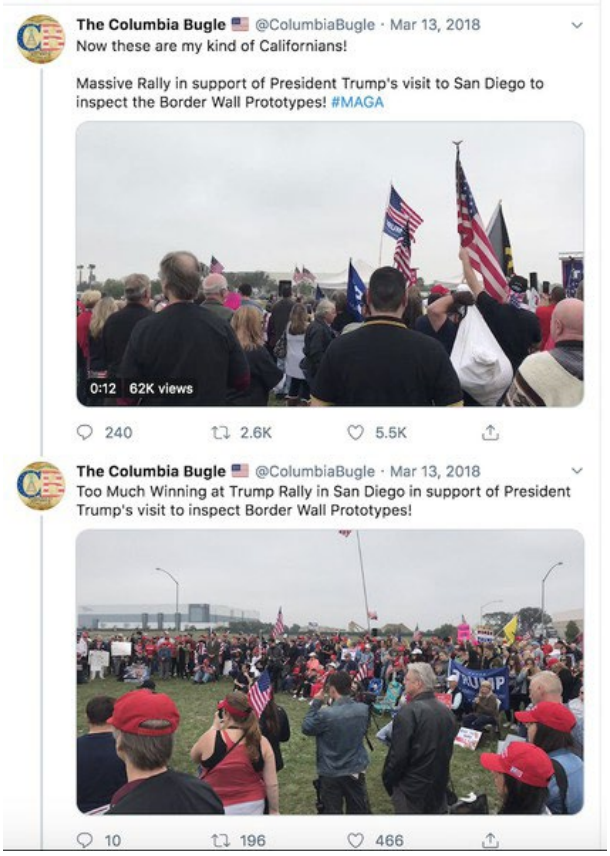
Преглед на алатките на ТвитБивер

Да го разгледаме, на пример, „Колумбија бјугл“ (The Columbia Bugle), популарен анонимен кориснички налог на крајната десница на Твитер, кој се пофали дека два пати бил ретвитуван од профилот на Доналд Трамп.

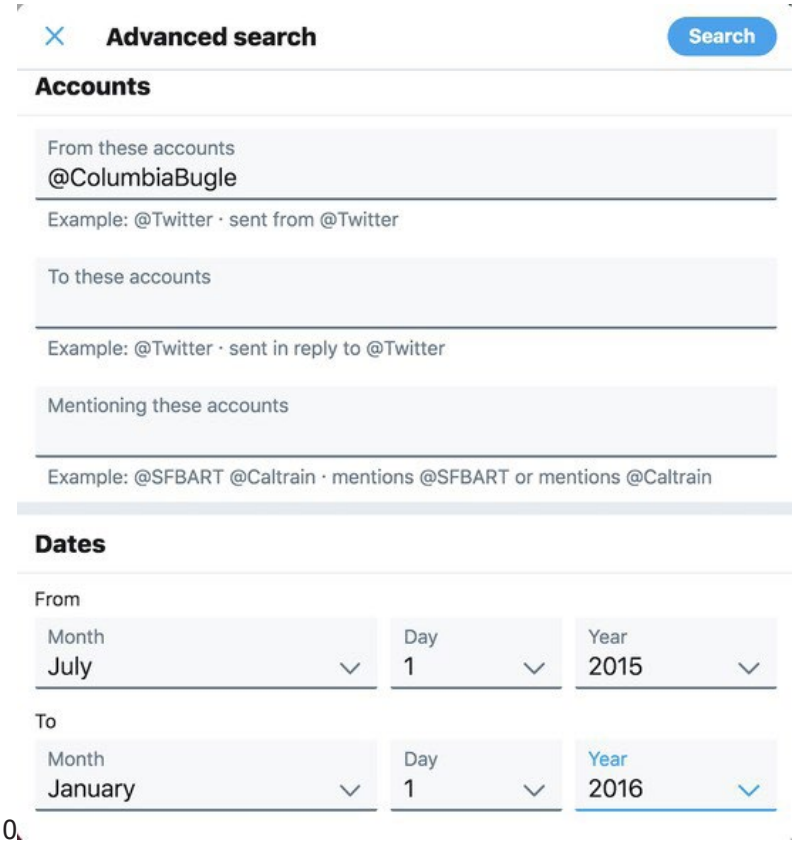


Најраните следбеници на Макс Деларџ (Max Delarge), корисник што тврди дека е уредник на „Колумбија Бјугл“, се извори на вести специфично посветени на Сан Диего, како и кориснички сметки посветени на спортот во Сан Диего. Бидејќи многу од твитовите објавени на Колумбија Бјугл вклучуваат видеа од митинзите на Трамп во Сан Диего, и настани поврзани со Универзитетот на Калифорнија во Сан Диего, можеме да бидеме доволно сигурни дека лицето што стои зад таа корисничка сметка живее во околината на Сан Диего.

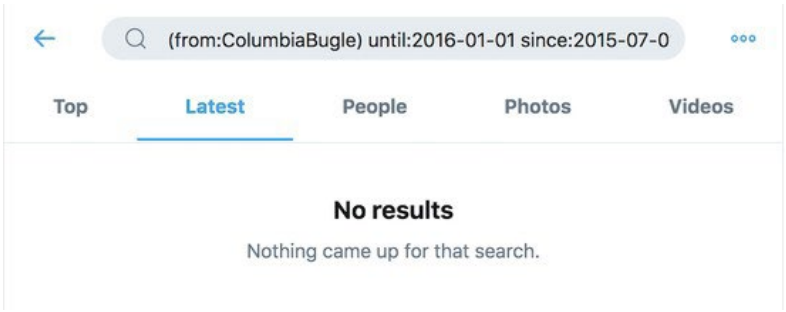




Кога почнувам нова истрага, сакам да почнам на почетокот на нечија историја на Твитер и да се движам нанапред низ хронологијата. Таму можете да стигнете рачно, со помош на авто-скролер (autoscroller) екстензијата на „Хром“, или можете да го искористите напредното пребарување на Твитер за да го ограничите периодот за преглед на првите неколку месеци од постоењето на корисничката сметка.



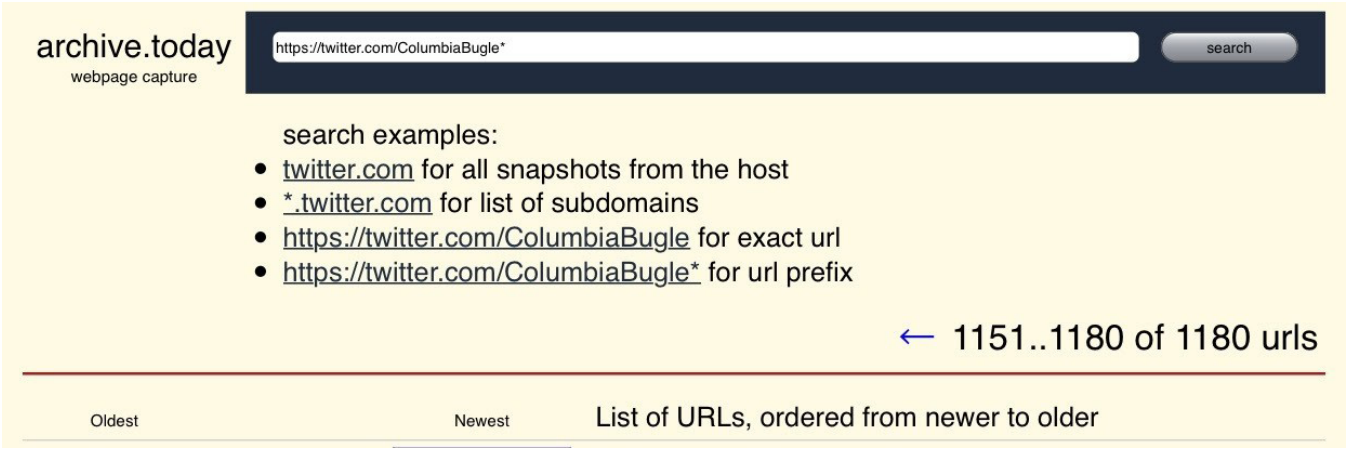
Помалку чудно, во првите шест месеци на оваа корисничка сметка резултатите беа нула твитови.



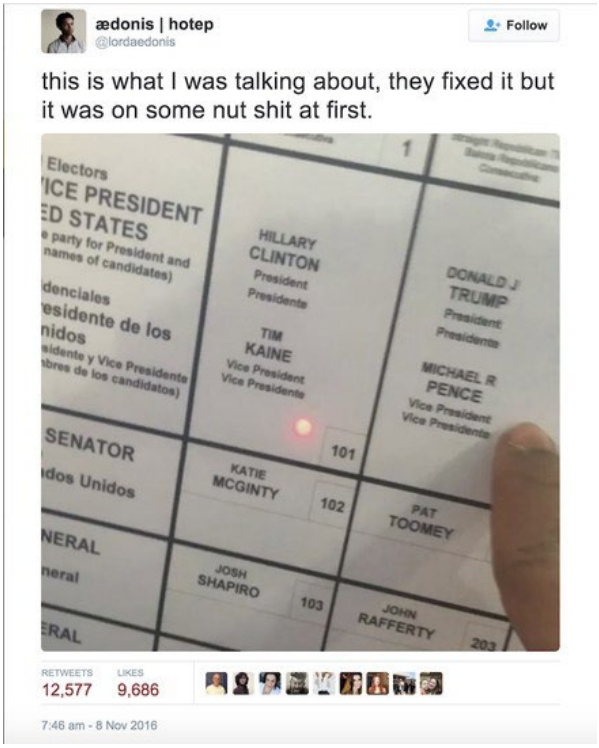
Тоа укажува на можноста лицето зад Колумбија Бјугл да ги избришало раните твитови. За да откријам какви биле тие твитови, можам да ги прилагодам критериумите за пребарување. Наместо твитови од сметката, ќе барам какви било твитови што го спомнуваат Колумбија Бјугл.

Тие конверзации потврдуваат дека „Колумбија Бјугл“ ги избришала сите твитови од првата година на постоењето, но не ни кажува зошто, а првите кориснички сметки со кои таа сметка влегла во интеракции не нудат многу сугестии.

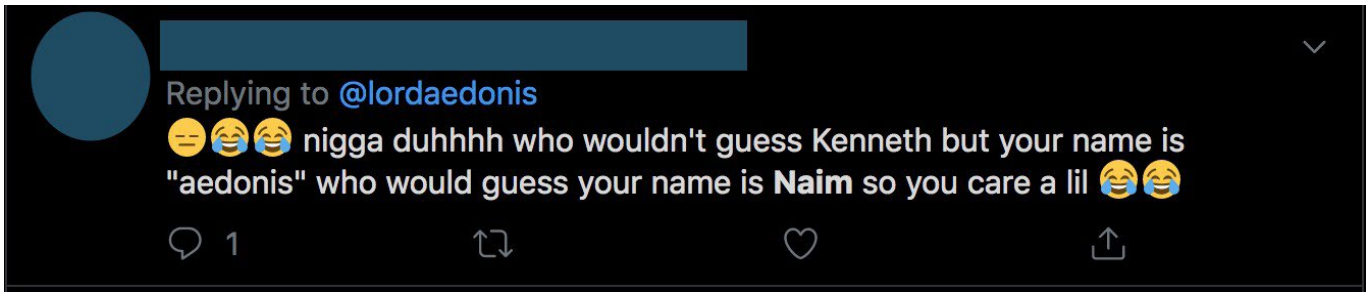
За да ги најдете неодамна избришаните твитови, можете да го пребарате „кешот“ (cache, ризница) на Гугл; постарите избришани твитови понекогаш се достапни на „Вејбек“ машината на „Интернет аркајв“ (Internet Archive›s Wayback Machine) или во други архиви. Архивската веб-страна archive.is, што се пополнува рачно, прикажа неколку избришани твитови од учеството на ColumbiaBugle на настан на кој студенти пишувале про-Трамп пораки на нивните универзитетски кампуси. За да ги видите сите твитови од таа сметка што некој можеби ги архивирал, како што јас направив за да го пронајдам овој твит, можете да пребарувате со префиксот на УРЛ адресата, користејќи астериск после името на сметката, на пример:



Ретко се случува некој успешно да го одвои својот реален живот од активноста во онлајн доменот. На пример, со еден колега од ЕнБиСи Њус (NBC News) ја раскажавме приказната за највиралното - и најлажливо - обвинување за изборна измама во 2016 година, со помош на еден сосед на десничарскиот трол што го твитуваше обвинувањето.



Иако твитот потекнуваше од човек познат на следбениците како @lordaedonis, луѓе од неговото соседство во реалниот свет одговарале на претходни твитови што ги објавил со вистинското име, што ги вклучивме во профилот на еден претприемач гладен за внимание чиј твит беше проширен од една сметка на твитер зад која стои Кремљ, и кој во крајна линија беше виден од милиони луѓе и промовиран од идниот претседател.

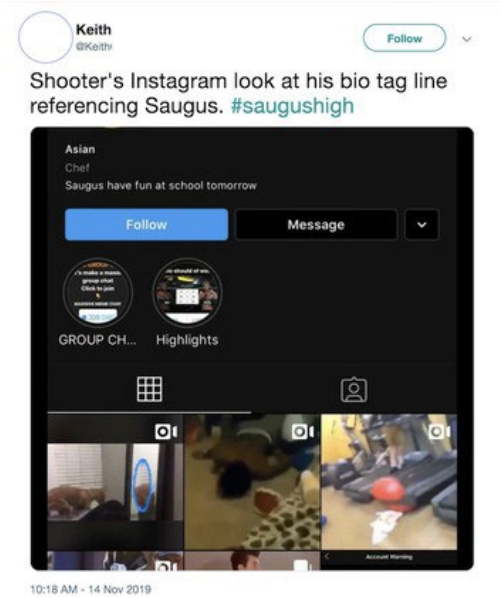


Омилени ми се приказните што ги откриваат вистинските луѓе зад влијателни, анонимни кориснички сметки на социјалните медиуми. Тие тајни кориснички сметки помалку зависат од алгоритмите и изработени се внимателно да служат како средство за бегство од јавниот живот. Тие овозможуваат да се остане во комуникација со семејството и пријателите одвоено од јавната корисничка сметка, или да се пренесуваат идеи и мислења што, од лични или политички причини, не смеат да ги кажат гласно.

Новинарката Ешли Фајнберг (Ashley Feinberg) е добрата вила на овој вид на сочни приказни што ги демаскираат алтернативните кориснички сметки на познати личности како што се Џејмс Коми (James Comey) или Мит Ромни (Mitt Romney). Нејзината тајна е едноставна и се состои од наоѓање на помалите сметки на членовите на нивните семејства што Коми и Ромни природно сакаат да ги следат, и прегледување на постовите во нив се додека не најде корисничка сметка што изгледа неавтентично но чија содржина и мрежа од пријатели/следбеници се совпаѓа со мрежите на овие реални личности.

Внимавајте на лажните кориснички сметки

Секоја од платформите си има свои карактеристики, способности за пребарување и начини на кои е полезна во различни ситуации кога настануваат вести. Сепак, имам едно предупредување во врска со корисничките сметки на социјалните медиуми: И кај нив е применливо правилото „верувај ама проверувај“. Постојат групи кои уживаат да си играат игри со новинарите. Особено во ситуации на вонредни вести, секогаш ќе се јавуваат нови лажни кориснички сметки, многу од нив со морничави или заканувачки постови наменети да ги привлечат новинарите. Следната лажна корисничка сметка на Инстаграм го користеше името на еден масовен убиец и беше отворена по нападот со огнено оружје во средното училиште „Corac“ (Saugus High School) во Калифорнија.. Таа привлече внимание преку „скрин-шотови“ објавени на Твитер, но Базфид Њус (BuzzFeed News) подоцна откри дека сметката не му припаѓа на напаѓачот.



Обезбедувањето потврда за една корисничка сметка од сопственикот, неговото семејство и пријателите, органите на прогонот и/или одделите за односи со јавност на социјалните медиумите е начин да се заштитите од можноста да бидете измамени.

Конечно, а веројатно и најзначајната забелешка: Не постои еден утврден и правилен редослед за завршување на наведените чекори. Често истрагата ме води во разни зајачки дупки и на мониторот имам отворено многу повеќе јазичиња со различни интернет-страници отколку што би сакала. Создавањето на систем што можете да го реплицирате - било да се работи за бележење на чекорите што сте ги направиле во документ на Гугл, или да платите комерцијална алатка како „Ханчли“ (Hunchly) да ве следи во пребарувањето - е клучно за разјаснување на врските помеѓу луѓето и нивните животи на интернет, како и за претворањето на заклучоците во приказни.

1а. Студија на случај: Како истражувањето на група кориснички сметки на Фејсбук откри оркестриран потфат за ширење пропаганда на Филипините

Авторка: Вернис Тантуко и Гема Багајаја-Мендоза

Гема Багајаја-Мендоза *(Gemma Bagayaua-Mendoza) работи како професионална новинарка 20 години, и сега го води одделението за истражувања и стратегија во „Раплер" (Rappler). Таа е предводник на одделот за проверка на факти и на истражувачкиот оддел за онлајн дезинформации и погрешни информации на Раплер.*

Вернис Тантуко *(Vernise Tantuco) е членка на истражувачкиот тим на Раплер и работи на проверка на факти и на истражување на мрежите за дезинформирање на Филипините.*

Есента 2016-та година, Џон Викторино (John Victorino), инвестициски аналитичар, му достави на Раплер листа од 26 кориснички сметки на Фејсбук од Филипините, за кои сметаше дека се сомнителни. Ние почнавме да истражуваме и да ги следиме тие кориснички сметки, и брзо откривме дека податоците наведени во нивните профили се лажни. Во текот на повеќенеделното истражување, тие 26 сметки не одведоа до откривање на многу поширока мрежа од страници, групи и кориснички сметки.

Сметките, заедно со една групација од страници и групи со кои беа поврзани, подоцна беа отстранети од Фејсбук. Тие на Раплер му послужија како инспирација да го создаде „Шарктенк" (Sharktank), алатка за следење на движењето на информациите на Фејсбук. Тие активности ја понудија основата за серија истражувачки приказни за начинот на кој пропагандните и оперативните операции на Фејсбук влијаат на демократијата во Филипините. Серијата вклучи и истражување на активностите на 26-те лажни кориснички сметки и го означи почетокот на нашето континуирано покривање на темата како Фејсбук е вепонизиран на Филипините за ширење на политички дезинформации, вознемирување на индивидуални лица и подривање на демократијата во земјата.

Оваа студија на случај се занимава со начинот на кој ги истражувавме изворните 26 сметки и како ги искористивме за да разоткриеме многу пошироки мрежи.

Верификување на идентитети, разоткривање на марионетите

Првиот чекор во истражувањето на групацијата кориснички сметки беше да потврдиме дали се поврзани со реални луѓе. Тоа бараше примена на старомодниот метод на проверка на факти што почна со крерање на табели во кои ги внесувавме деталите поврзани со сметките, вклучувајќи ги наведените лични податоци, страниците што означиле дека им се допаѓаат и други информации.

На пример, корисникот на Фејсбук Мутја Баутиста (Mutya Bautista) самата се опишува како „аналитичар за софтвер“ во ЕјБиЕс-СиБиЕн (ABS-CBN), најголемата телевизиска мрежа во Филипините. Раплер ги провери тие наводи во ЕјБиЕс-СиБиЕн, и тие потврдија дека такво лице не е вработено кај нив.

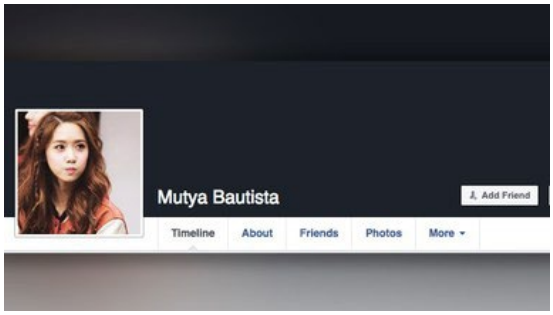
Personal Information	
Facebook ID	https://www.facebook.com/profile.php?id=10
Profile Name	Mutya Bautista
Occupation	Software Analyst
Current Company	ABS-CBN Corporation
Former Occupation 1	
Former Occupation 2	
Former Occupation 3	
Former Occupation 4	
Former Occupation 5	
Studied	Computer Engineering
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	

Со алатки за реверзибилно пребарување на слики, откривме дека повеќето од 26-те сметки користеа профилни слики од познати и славни личности.

Баутиста, на пример, користеше слика од Им Јуна (Im Yoona) членка на корејската поп група „Грлс џенерејшн“ (Girl’s Generation). Сметката на Лили Лопез (Lily Lopez), прикажана подолу, користеше слика од корејската актерка Ким Саранг (Kim Sa-rang).



Друга корисничка сметка, „Лувимин Кансио“ (Luvimin Cancio), користеше слика преземена од softcorecams.com, порнографска веб-страница, како своја профилна фотографија. Ја идентификувавме таа веб-страница како извор на фотографијата преку алатката за реверзибилно пребарување на слики „Тинај“ (TinEye).

Корисничките сметки често користеа слични насловни фотографии на своите профили. Подолу ја имате насловната фотографија од сметката на Јасмин дела Торе (Jasmin De La Torre), иста како и на сметката на Лили Лопез (Lily Lopez).

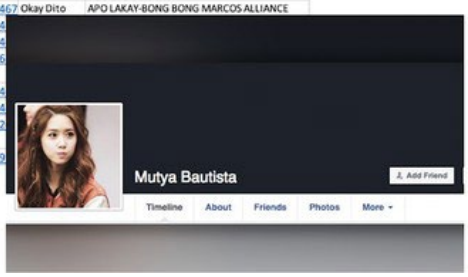
Забележавме уште една интересна работа за 26-те сметки: Тие корисници имаа повеќе групи во кои членуваат од пријатели на Фејсбук.

Тоа е необично, затоа што повеќето Филипинци имаат пријатели или роднини во странство. Фејсбук, во основа, служи како комуникациски канал преку кој луѓето одржуваат контакти со роднините и пријателите. Тенденцијата е да имаат многу пријатели а не да членуваат во голем број групи.

Листата на пријатели на Баутиста, која тогаш беше јавна, покажуваше дека таа имаше само 17 пријатели. Всушност, секоја од 26-те кориснички сметки што ги идентификувавме имаше помалку од 50 пријатели во моментот кога ги откривме, во 2016-та година.

Од друга страна, Баутиста членуваше во повеќе од сто групи, вклучувајќи и групи вклучени во кампањата на тогашниот кандидат за потпретседател на државата Фердинанд Маркос Помладиот (Ferdinand Marcos Jr.), неколку групи на Филипинци што живеат во странство, како и групи за купопродажба. Сите тие групи имаа членство од неколку десетици до неколку стотици илјади членови. Сите заедно, тие групи имаа повеќе од 2,3 милиони членови на Фејсбук. Подолу е дадена листа на некои од најголемите групи, со бројот на нивните членови. Наведена е и листа на постовите што Баутиста ги поставила на тие групи.

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/OFWnewgei	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 J	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		



Со комбинација на сите наоди и поврзаните податоци, заклучивме дека тие кориснички сметки се марионети: Фиктивни идентитети создадени за да поддржат одреден став.

Про-Маркос мрежа

Од датумите на кои биле поставени профилните фотографии и раните постови на 26-те сметки можевме да видиме дека биле создадени во последниот квартал од 2015-та година, во пресрет на изборите од мај 2016-та година. Исто така, откривме дека конзистентно промовираат содржини што ги негираат документираните злоупотреби на воената состојба во 1970-те години, за време на режимот на Маркос. Тие кориснички сметки ги напаѓаа ривалите на синот на поранешниот диктатор, кандидатот за потпретседател на државата Фердинанд „Бонгбонг“ Маркос Помладиот.

Во следниот пример, корисничката Мутја Баутиста сподели едно, во меѓувреме раскринкано, тврдење дека ривалот на Бонгбонг - во тој момент новопрогласениот потпретседател Лени Робредо (Leni Robredo) - бил оженет со една активистка пред таа да се омажи по втор пат за починатиот министер за внатрешни работи и локална управа Џеси Робредо (Jesse Robredo). Баутиста ја постави приказната со наслов “Дали Лени Робредо бил оженет со анти-Маркос тинејџерка пред таа да го запознае Џеси?“ на групата „Про-Бонгбонг Маркос Интернешенал Пауер“ (Pro Bongbong Marcos International Power», со коментар: “*Kaya ga-nun na lamang ang pamemersonal kay [Bongbong Marcos], may root cause pala.*” („Затоа е насочено против личноста на [Bongbong Marcos], тоа е изворната причина.”)

Друга сомнителна сметка со име Раден Алфаро Пајас (Raden Alfaro Payas) ја сподели истата статија на групата „Фејсбук воини лојални на Бонгбонг Маркос“ (Bongbong Marcos loyalist Facebook warriors) со истата легенда - од збор до збор, со истата интерпункција - истиот ден.

Лажни кориснички сметки често се користат за спамирање на групи со линкови, а понекогаш можете да ги фатите во користење на идентичен текст при споделувањето. Во тоа време уште можеше да се користи пребарувањето „Facebook Graph“ за преглед на јавните постови на корисниците што членуваат во групите. Сепак, Фејсбук укина многу од можностите за пребарување „Graph search“ во 2019 година, вклучително и таа функционалност. Резултат на тоа е што денес треба да влезете во групите и да пребарувате за да видите што споделувале индивидуалните корисници.

Поврзани веб-страници

Анализата на содржините што ги споделувале корисничките сметки ни овозможи да сфатиме дека 26-те марионети ги промовираа истите веб-страници: „Океј Дито“ (Okay Dito (OKD2.com)), „Прашајте ги Филипините“ (Ask Philippines (askphilippines.com)) и why0why.com, помеѓу другите.

OKD2.com објави повеќе измами и други пропагандни материјали во полза на семејството Маркос и на претседателот Родриго Дутерте (Rodrigo Duterte). Денес функционира маскирано како веб-страница за мали огласи. Но, во септември 2016 година откривме дека содржините од веб-страницата биле споделени 11,900 пати на Фејсбук, делумно благодарение на марионетите.

Преку тие веб-страници, Раплер конечно дојде до можниот одговор кој ги влече конците зад 26-те кориснички сметки: лице со име Раден Алфаро Пајас.

Следење на кукларите

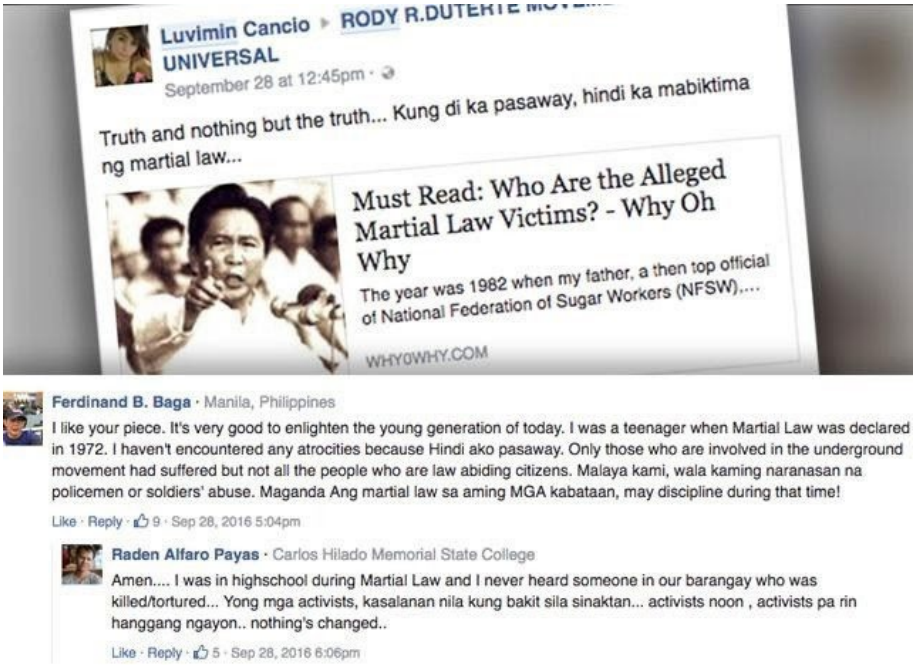
Како и многу други веб-страници што ги набљудува Раплер, записите за регистрацијата на сегашниот домен на OKD2.com не се достапни за јавноста. Веб-страната не ги открива имињата на авторите со кои соработува или на сопсвениците, и не нуди други информации за контакт освен онлајн формулар за испраќање на електронска пошта.

За среќа, можевме да ги искористиме историските записи за сопственоста на доменот за да го идентификуваме лицето поврзано со веб-страната. Со користење на страната domain-tools.com, дознавме дека, почнувајќи од јули 2015 година, OKD2.com е регистриран на извесен Раден Пајас, жител на Танауан Сити, Батангас (Tanauan City, Batangas). Откривме и дека OKD2.com го дели истиот идентификациски број на „Гугл Адсенс“ (Google AdSense) со други веб-

страници, како што се askphilippines.com и why0why.com, споделувани на 26-те кориснички сметки. Идентификациските броеви на „АдСенс“ на овие веб-страници ги откривме преку преглед на нивниот изворен код, барајќи серии бројки што почнуваат со буквите „ca-pub-“. Сите сметки на „Гугл АдСенс“ добиваат единствен идентификациски број што почнува со „ca-pub-“, а секоја страница на некој веб-сајт што е поврзан со сметката го содржи овој идентификациски број.

Заедно со записите за доменот, увидовме дека една од 26-те кориснички сметки го носеше името Раден Алфаро Пајас (неофицијално). Откривме уште една корисничка сметка на негово име со корисничкото име „realradenpajas“, што имала контакти со некои од марионетите.

На пример, тој коментирал на еден пост на Лувимин Канцио на кој имало линк до приказна што ги негора злоделата направени за време на воената состојба прогласена во периодот кога Маркос ја имаше власта. Според „вистинската“ корисничка сметка на Пајас, тој бил средношколец додека траела воената состојба и „никогаш не слушнал“ дека некој бил убиен или измачуван.



Покренување на „Шарктенк“

26-те лажни кориснички сметки и нивниот досег го инспирираа Раплер да ја креира базата на податоци „Шарктенк“ (Sharktank, базен со ајкули) и да го автоматизира собирањето на податоци од јавните групи и страници на Фејсбук. До август 2019 година, Раплер следеше околу 40,000 страни со милиони следбеници.

Она што почна како истрага на група сомнителни кориснички сметки се претвори во континуирана студија на една мрежа од илјадници лажни и вистински сметки, групи и страници што шират дезинформации и пропаганда, ја дисторзираат политиката и ја ослабуваат демократијата на една нација.

1б. Студија на случај: Како докажавме дека најголемата Фејсбук-страница посветена на БЛМ (Black Lives Matter) е лажна

Автор: Дони О'Саливен (Donie O'Sullivan)

Дони О'Саливен *е репортер на СиЕнЕН што ги покрива темите во кои се сечат технологијата и политиката. Тој е дел од тимот „СиЕнЕн Бизнис" (CNN Business Team) и соработува со истражувачката единица на СиЕнЕн во следењето и идентификацијата на дезинформативните кампањи на интернет што за цел го имаат американскиот електорат.*

Летото и есента 2017 година, како што светот почна да дознава повеќе детали за обемните напори на Русија да влијае врз американските гласачи преку социјалните медиуми, стана јасно дека Афро-американците и движењето „Црните животи се важни" се помеѓу главните цели на кампањата за ширење раздор на Кремљ.

Со моите колеги од СиЕнЕн со месеци известувавме како Русија стои зад некои од најголемите кориснички мрежи на „Црните животи се важни" (БЛМ) на социјалните медиуми. Кога разговарав со активисти на БЛМ (BLM - Black Lives Matter), понекогаш ќе ми го поставеа прашањето „Знаеш ли кој ја води најголемата БЛМ страница на Фејсбук?"

За неверување, никој - вклучувајќи ги и најпознатите активисти на БЛМ во земјата и организатори што работат на терен - не го знаеше одговорот. Разбирливо, некои се сомневаа дека страната можеби е управувана од Русија. Но нашата истрага откри дека не е руска, не е ниту американска - страницата ја водеше бел човек од Австралија.

Страницата, едноставно насловена „Black Lives Matter", изгледаше дека е легитимна. До Април 2018 година таа имаше безмалку 700,000 следбеници. Постојано споделуваше линкови до приказни за полициската бруталност и нееднаквоста; спроведуваше онлајн акции за собирање на фондови; дури имаше и онлајн продавница што продаваше производи брендирани од БЛМ.

Воопшто не е невообичаено страница со такви димензии да биде водена анонимно. Некои активисти не сакаат нивното име да се појави на страницата и да ризикуваат да го привлечат вниманието на тролови или на органите на прогонот што сакаат да ги задушат протестите. Надвор од САД, способноста на активистите да водат страници чувајќи ја анонимноста беше од огромно значење за дигиталниот активизам и основата за постоењето на некои движења. (И токму тоа го искористи Русија, засилувајќи ги сомнежите поврзани со оваа БЛМ страница.)

Само што почнав да обрнувам внимание на таа мистериозна страница, Џереми Маслер (Jeremy Massler), слободен истражувач и одличен онлајн детектив, ме контактираше со една иницијална информација. Маслер ги прегледувал записите за регистрација на домени на веб-страниците кон кои постојано линкуваше таа голема Фејсбук страница на БЛМ. Иако домените беа регистрирани со целосно почитување на приватноста, открил дека еден од нив, во еден краток временски период во 2016 година, му припаѓал на Иан Меккеј (Ian MacKay) од Перт, Австралија - и белец.

```
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
```

Маслер го контактирал Меккеј кој му кажал дека тој купувал и продавал домени како хоби и дека нема никаква врска со страницата на Фејсбук. Меккеј, средовечен синдикалист, ми го даде истото објаснување и мене кога го контактирав по телефон неколку месеци подоцна. Дотогаш веќе знаевме дека Меккеј регистрирал десетици имиња на веб-страници, многу од нив поврзани со црнечкиот активизам.

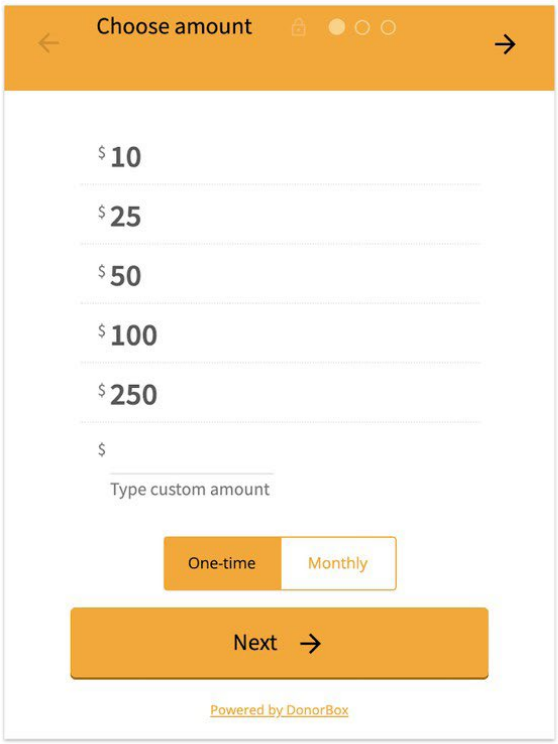
Наспроти загриженоста околу страницата и фактот дека неколку активисти ми кажаа дека имаат сомнежи за неа, не сметав дека објаснувањето на Меккеј е неверојатно. Имињата на домени можат да имаат голема вредност и луѓето цело време се занимаваат со нивно купување и продавање. Фактот дека тој регистрирал и продавал домени што не беа поврзани со прашањето на црнечкиот активизам ги правеа неговите тврдења уште поверодостојни. Но, тогаш се случи нешто чудно. Неколку минути откако зборував со Меккеј, страницата на Фејсбук „падна“. Не беше отстранета од Фејсбук, туку од кој и да е што ја водеше - и не беше целосно избришана туку само привремено отстранета.

Тоа изгледаше мошне сомнително па продолживме да копаме со Маслер.

Страницата на Фејсбук, што се врати онлајн неколку недели по мојот телефонски разговор со Меккеј, во своето постоење промовирала кампањи за собирање на финансиски средства, претпоставка е, за каузи поврзани со БЛМ.

За една таква кампања, тврдеше дека собира пари за активистите од Мемфис, Тенеси. Но, кога зборував со тамошните активисти, никој не знаеше ништо за кампањата или каде можеби се отидени тие пари. Други активисти дури ни кажаа дека ја пријавиле страницата до Фејсбук, поради сомнеж дека се работи за измама. Но, компанијата не преземала никакви дејства по тоа прашање.

Black Lives Matter



Thank you for taking a look at this page, We appreciate all donations and all proceeds go toward Black Lives Matter Media campaigns which is an amazing cause aimed at bringing media attention to Racism and Bigotry. We are not sponsored or funded by any other part of the BLM movement or big companies or celebrities and we soley rely on the kindness of every day supporters like you. So far we have posted over 30 000 news stories and had literally millions of visits to the website www.blacklivesmatter1.com , grown our Facebook page to over 360 000 supporters www.facebook.com/blacklivesmatter1and we have a reach of up to 8 million people a week who see the most confronting stories of injustice to Black people. We want to reach even more people so our children might not have to suffer racism in the way we do now in the future. This movement was formed by the people and is being moved forward by the people. We have largely funded this ourselves and we are a very, very small crew. It is becoming a struggle to keep going so we have decided to see if people are willing to get behind us and help. We understand a lot of people are doing it tough, if you are you can still help by sharing this page to others. Thank you so much!

Кога ги контактирав бројните платформи за онлајн плаќања и собирање на финансии што ги користела страницата, компаниите што стојат за тие платформи почнаа да ги отстрануваат кампањите за собирање средства со објаснување дека ги прекршиле нивните правила. Повикувајќи се на заштитата на приватноста на корисниците, ниту една од тие компании не ми даде официјална информација каде одеа парите. Тоа е предизвик со кој често се соочуваме. Повикувајќи се на политиките за заштита на приватноста, дигиталните платформи и сервиси ретко им ги откриваат на медиумите имињата или информациите за контакт на носителите на кориснички сметки.

Подоцна дознав од еден извор што е запознаен со некои од процесираните уплати дека барем една од сметките е поврзана со банкарска сметка и ИП (IP) адреса во Австралија. Друг извор ми кажа дека биле собрани околу 100,000 долари.
Негувањето на извори во технолошките компании кои ќе сакаат да ви дадат повеќе информации од што компанијата би ви кажала во камера станува сè позначајно затоа што многу стории не можат да бидат разоткриени само со користење на отворени извори, особено затоа што измамниците и злонамерните актери се сè пософистицирани.

Со тие информации отидов во Фејсбук по коментар за приказната и им кажав кеда имам докази дека страницата има врска со Австралија, дека платежните компании ги отстранија кампањите по нивната истрага, и дека знаеме дека барем дел од парите одат во Австралија. Гласноговорникот на Фејсбук одговори дека истрагате спроведена од платформата за социјален медиум „не покажа ништо што ги повредило нашите Стандарди на заедницата“ (Community Standards).

Малку пред да ја објавиме приказната - и само откако на еден вработен во Фејсбук на повисока позиција во компанијата му изразив загриженост за истрагата на Фесјбук и одговорот на нивниот гласноговорник - Фејсбук конечно дејствуваше и ја отстрани таа страница од платформата.

Австралискиот синдикат во кој работеше Меккеј започна своја истрага по објавувањето на извештајот на СиЕнЕн. Нецела недела подоцна, Меккеј беше отпуштен од работа а синдикатот објави дека уште еден нивни службеник е вклучен во измамата.

Она што треба особено да се забележи кај оваа приказна е широкиот дијапазон на техники што ги употребивме со Маслер за да стигнеме до целта. Се потпиравме на веб-страници за архивирање како што е „Вејбек Машин“ (Wayback Machine) што ни овозможуваше да видиме како изгледаат веб-страниците кон кои линкуваше страната на Фејсбук, како и самата страна пред да ни „излезе на радарот“. Тоа се покажа особено корисно затоа што, откако Маслер го оствари првиот контакт со Меккеј, луѓето што стоеја зад страната на Фејсбук се обидоа да прикријат некои од своите траги.

Користевме и услуги за следење на регистрациите на домени, вклучувајќи го и DomainTools.com, за истражување на веб-страниците што ги регистрирал Меккеј и да ги пронајдеме податоците за директен контакт со него. Маслер многу го користеше пребарувањето „Фејсбук граф“ (алатка што веќе не е достапна) за следење на лажните профилни сметки на Фејсбук што биле воспоставени за промоција на страната во „Фејсбук групс“ (Facebook Groups). Прегледувањето на информации од отворени извори и користењето на онлајн алатки за истражување, како оние што ги користевме за да пристапиме до записите за домените, се од витално значење - но, не се единствените алатки што можат да се искористат.

Едноставниот разговор по телефон со Меккеј и развојот на извори за да стигнеме до информации што инаку не би биле јавни - традиционални новинарски техники - беа клучни во расветлувањето на оваа измама.

2. Откривање на нултиот пациент

Автор: Хенк ван Ес

Хенк ван Ес *(Henk van Ess) е проценувач во Меѓународната мрежа за проверка на податоци на Поинтер (Poynter's International Fact-Checking Network). Барањето на приказни во чистите податоци е негова опсесија. Ван Ес обучува медиумски работници од целиот свет во областа на истражувањето на интернет, социјалните медиуми и мултимедијалните содржини. Меѓу неговите клиенти се и ЕнБиСи Њус (NBC News), Базфид Њус (BuzzFeed News), Глобал витнес (Global Witness), СРФ (SRF), Аксел Шпрингер (Axel Springer), бројни НВО и универзитети. Неговите веб-страници whopostedwhat.com и graph.tips се нашироко користени за филтрирање на социјалните медиуми. На Твитер можете да го пронајдете како @henkvaness.*

Канадскиот стјуард Гаетан Дуга (Gaëtan Dugas) со децении беше познат како „Нулти пациент", човекот што прв го донесе вирусот на ХИВ/СИДА во САД. Тоа признание, засилено во многуте книги, филмови и безбројните новински извештаи, од него направи „архи-душман од една епидемија која, во крајна линија, ќе убие повеќе од 700,000 луѓе во Северна Америка".

Но не беше баш така. Бил Дероу (Bill Darrow), истражувач на Центрите за контрола и превенција на болести (Centers for Disease Control and Prevention), го интервјуирал Дуга и го завел во архивата како „Пациент О", како „Од Калифорнија". Наскоро тоа било погрешно прочитано како бројката 0, започнувајќи верижна реакција на погрешна информација што траеше до неодамна.

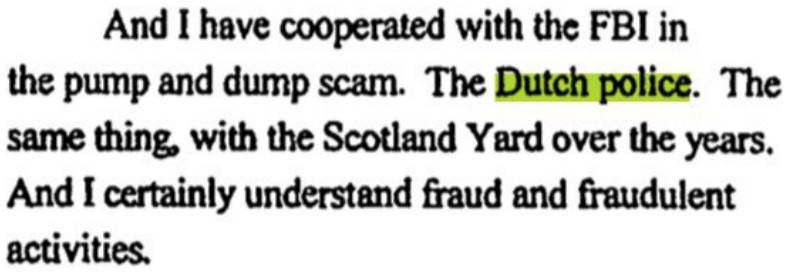
Можно е и новинар да се фокусира на погрешен нулти пациент ако не знае како правилно да пребарува. Ова поглавје ќе ви помогне да ги пронајдете примарните онлајн извори со отстранување на површните резултати и подлабоко „копање".

1. Ризици при консултирањето на примарни извори и како да ги избегнете

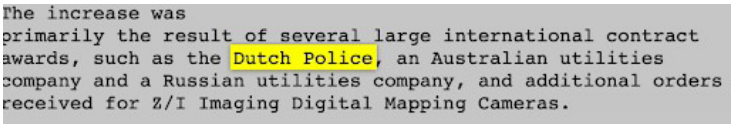
Новинарите ги љубат примарните онлајн извори. Докази од прва рака можат да се најдат во новинска статија, во научна студија, во изјава за медиумите, на социјалните медиуми или на кој било друг „нулти пациент".

Спроведувањето на основно пребарување со клучни зборови на некоја официјална веб-страница на владата може да ве доведе да помислите дека „она што го гледате е тоа што го имаат". А тоа често не е точно. Еве ви еден пример. Да одиме на интернет страната на Комисијата за хартии од вредност на САД (U.S. Securities and Exchange Commission), извор што се користи за наоѓање финансиски информации за граѓаните на САД, но и за деловни луѓе од целиот свет. Да замислиме дека сакаме да го пронајдеме првото појавување на фразата „Dutch police" (Холандска полиција) на страната sec.gov. Вградениот пребарувач на СЕЦ може да помогне:

Има само еден пронајден документ, од 2016 година. Значи, СЕЦ ја спомнува холандската полиција само еднаш, во 2016 година, така?


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.

Погрешно. Првото спомнување на sec.gov е 12 години порано, во 2004 година, во една декласифицирана, шифрирана електронска порака:


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.

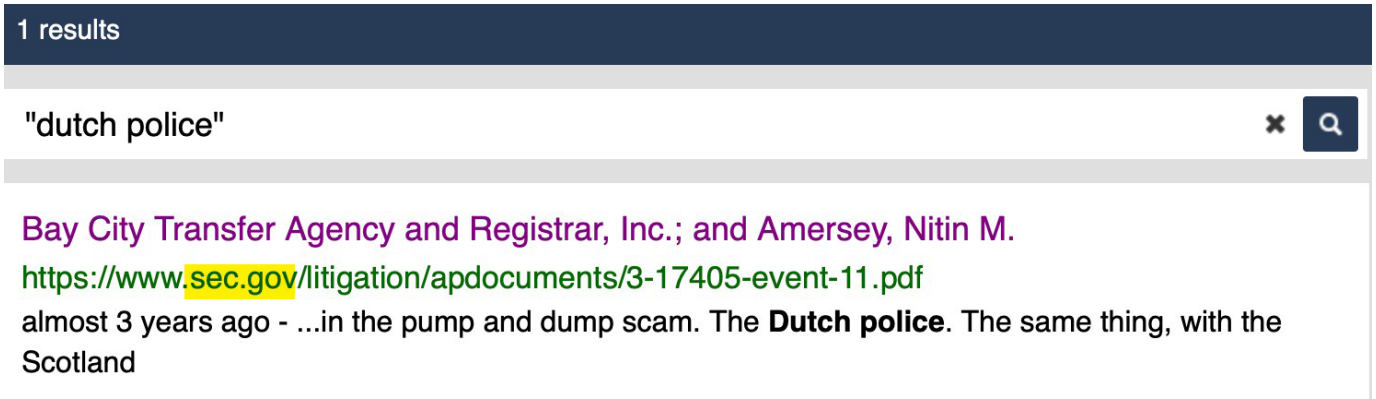
Тоа нема да го видите во резултатите од пребарувањето на sec.gov, иако таа информација доаѓа токму од нивната веб-страница. Зошто се јавува таква разлика?

Скоро по дефиниција, не треба да им верувате на пребарувачите на примарните извори. Тие можат да создадат лажен впечаток за содржината на веб-страната и со неа поврзаните бази на податоци. Правилен начин на пребарување е да „проверката на примарниот извор“.

Проверка на примарен извор

Чекор 1: Погледнете го линкот што не функционира

Резултатите од пребарувањето на СЕЦ ни дадоа само еден извор:



Да се позанимаваме со тоа разочарување. Прво, да го отстраниме делот „https://www», првиот дел од линкот. Барајте ја првата коса црта по (/) - во нашиот случај пред зборот „litigation/»

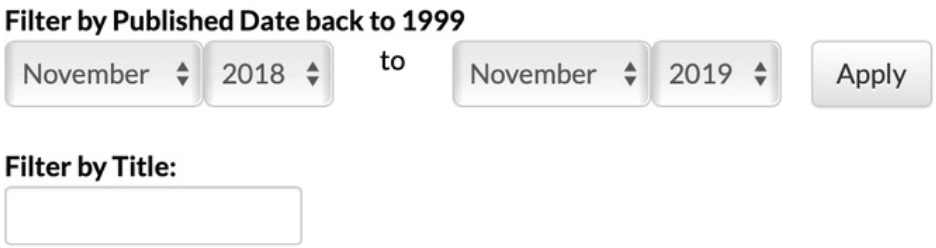
Тоа е делот што ни треба: sec.gov

2. *Втор чекор: Користете „site“:*

Одете на некој генерички пребарувач. Почнете со фразата („Dutch police») и завршете со „site»: По што треба да ја внесете УРЛ адресата (без празно место). Тоа е формулата за да видите дали некој оригинален извор ви прикажува сè:

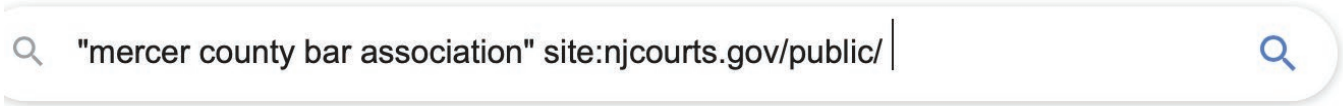
Вклучување на специфични папки

Сега можете да ја прилагодите „формулата за примарен извор“ на вашите специфични потреби. Да појдеме во рубриката за изјави за медиумите на веб-страната на Судовите на Њу Џерси (New Jersey Courts). Да претпоставиме дека сакате да дознаете кога Адвокатската комора на округот Мерсер (Mercer County Bar Association) спонзорирала програма за „Денот на законот“ (Law Day), но не можете да го пронајдете примарниот извор во насловот на ниту една изјава за медиумитеу. Комората „Mercer County Bar Association“ не е наведена во ниту еден од насловите.



Сега погледнете ја УРЛ адресата на таа страница преполна со лошо индексирани изјави за медиуми:

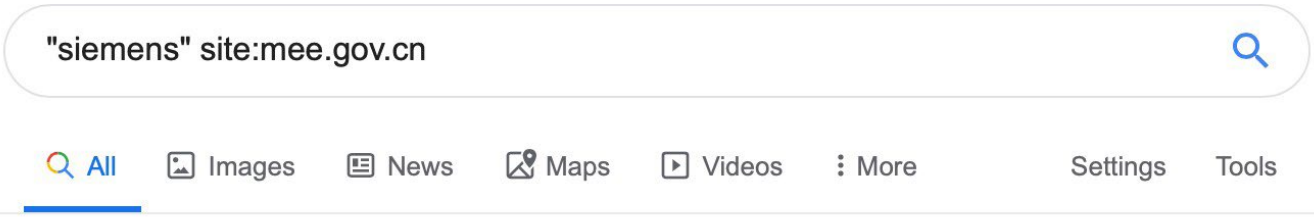
Материјалите што се однесуваат на односите со јавноста се чуваат во папката /public. Тоа треба да биде вклучено во вашите критериуми за пребарување на Гугл:



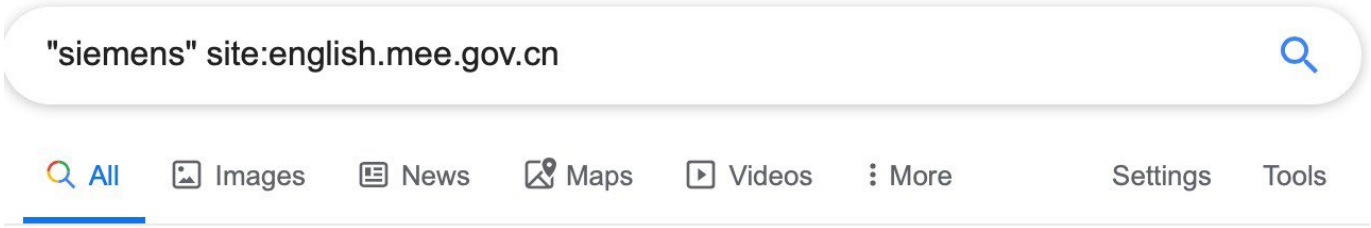
Значи, еве како треба да изгледа:

Предвидување на имињата на папките

Кина има Министерство за екологија и животна средина. Дали тоа министерство поседува документи на англиски јазик за германската компанија „Сименс“ (Siemens)? Со примена на следната формула, во резултатите од пребарувањето добивате документи и на кинески и на англиски јазик:



Ако сакате да ги филтрирате резултатите за да ги видите само документите на англиски јазик, можеби тие го употребиле зборот „English“ во линкот? Обидете се. Успеа:



2. Следење на трагата на документите

Понекогаш, информацијата што ни треба не се наоѓа на некоја веб-страница, туку во посебен документ чуван на таа веб-страница. На следниот начин можете да ја следите трагата на документот со користење на формулите на Гугл.

Рос Мекитрик (Ross McKitrick) е вонреден професор на Катедрата за економија на Универзитетот Гуелф, во Онтарио, Канада. Во 2014 година, тој одржа презентација за една група климатски скептици. Да се обидеме да ја пронајдеме поканата за таа средба. Знаеме дека настанот се одржал на 13 мај, 2014 година, на 11-от Годишен работен ручек организиран од „Пријателите на науката“ (Friends of Science (FOS)). Ако тие термини ги пребараме на Гугл, нема да добиеме никакви резултати:

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

Зошто? Затоа што зборот *„invitation*" (покана) не се спомнува во многу покани. Истото се случува со зборот *„interview".* Многу интервјуа не го содржат зборот *„interview"*. Дури и на мнозинството географски карти никаде експлицитно не пишува „географска карта“. Што би ве советувал? Престанете со нагаѓање и пробајте со „Зен“ приод.

Чекор 1: Утврдете за каков вид на документ се работи

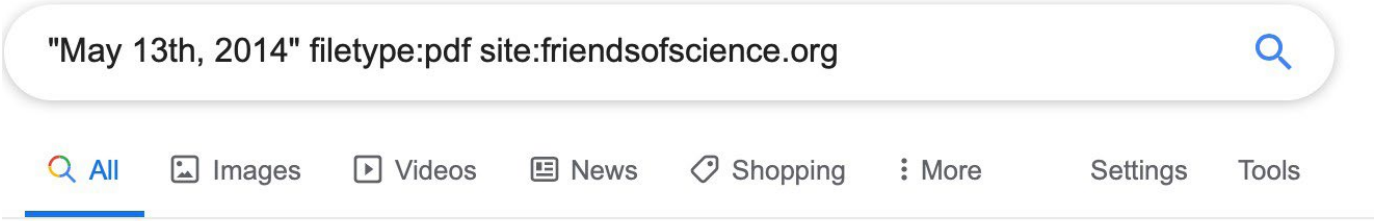
Обидете се да го пронајдете заедничкиот именител за сите онлајн покани. Најчесто се работи за ПДФ (PDF) документи. Пребарајте со токму тој критериум, користејќи ја фразата за пребарување „filetype:pdf“ и можеби ќе ја пронајдете поканата.

Чекор 2: Бидете (климатски) неутрални

Не го знаете точниот текст на поканата. Она што знаете е дека видеото објавено на Јутјуб (YouTube) е од настан одржан на 13.05.2014 година. Можно е датумот да бил спомнат во поканата. (Секако проверете ги двете форми за пишување на датум, 13-ти мај, и 13.05.)

Чекор 3: Кој е организатор?

Знаеме дека настанот е организиран од „Пријатели на науката“, а нивната веб-страница е friendsofscience.org. Ако ги комбинираме сите три чекори, линијата за пребарување во Гугл ќе гласи:



Ете ја во првиот излистан резултат: поканата за настанот.

ФОС, со седиште во Калгари, често е означена како група што ја негира климатската криза, а делумно е финансирана од индустријата за нафта и гас. Како да ја формулираме линијата за пребарување за да пронајдеме повеќе информации за групата и за нејзината мрежа од поддржувачи и финансиери?

Чекор 1: Вклучете ја целта

Фразата „Friends of Science“ прикажува премногу резултати, па вклучете го и зборот „Calgary“ во пребарувањето. Чекор

Чекор 2: Вклучете ја фразата „filetype#

Пробајте со најдобрата опција за каков било официјален документ, „filetype:pdf“.

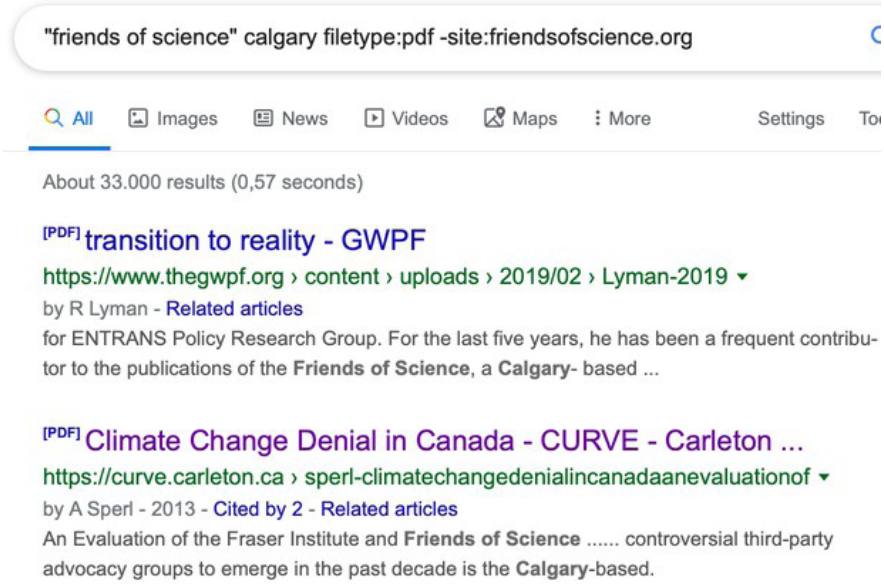
Чекор 3: Исклучете ја веб-страницата на вашата цел

Исклучете ја од пребарувањето веб-страната Friendsofscience.org со додавање на линијата „-site:friendsofscience.org». Тоа ќе ви помогне да пронајдете информации од трети страни.

Целата линија за пребарување гласи:

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

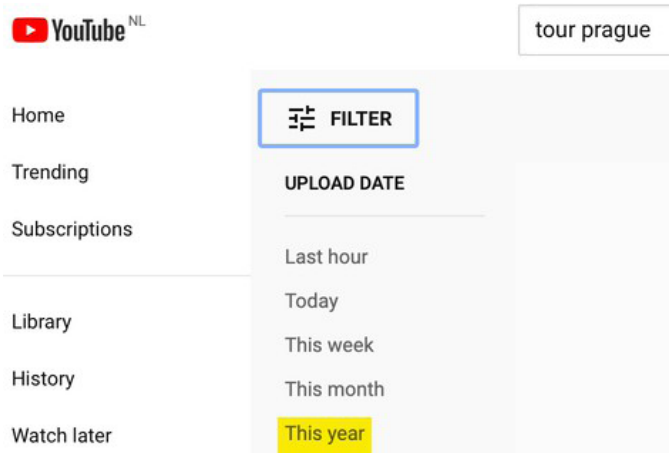
Бидејќи пребарувавте во официјални документи, но не на нивната веб-страна, пронајдовте некои од „соборците“ на организацијата и луѓе што ја критикуваат:



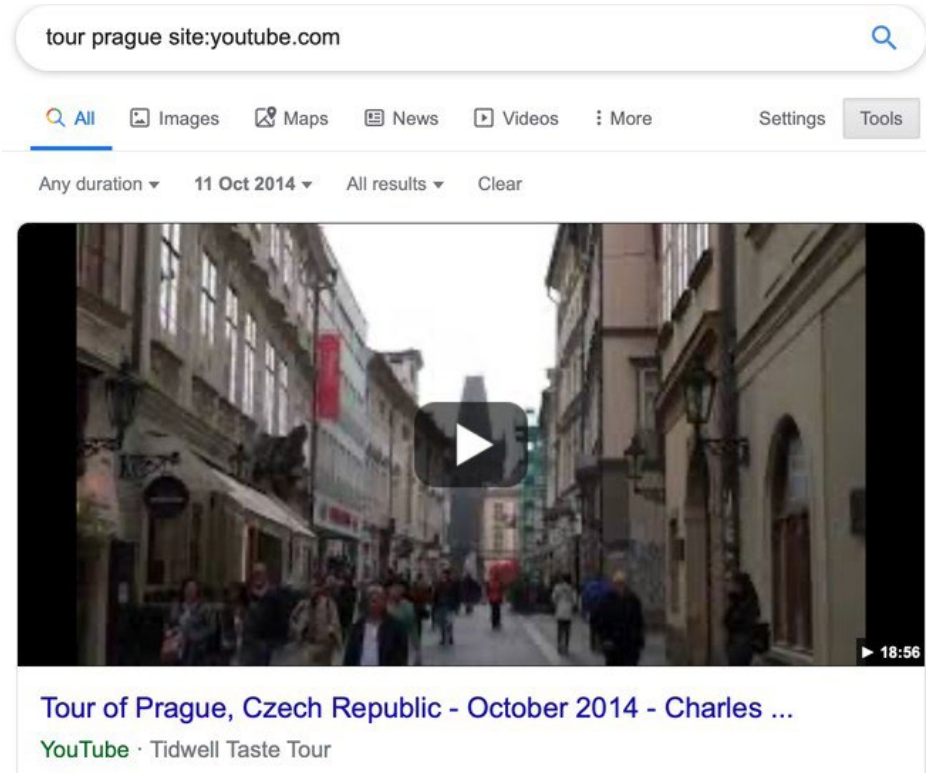
3. **Филтрирање на социјалните медиуми за наоѓање на примарни извори**

Јутјуб (YouTube)

Алатката за пребарување на Јутјуб има еден проблем: не дозволува филтрирање за да пронајдете видеа што се постари од една година. Ако, на пример, сакате да пронајдете видео од туристичко разгледување на Прага снимено на 11.10.2014 година, ќе наидете на следната пречка:



За да го решите проблемот, рачно внесете го посакуваниот датум во Google.com со користење на менито „Tools“ на крајната десна страна. Изберете ги опциите „Any time» (Кое било време) и „Custom Range“ (Избран опсег). Сега ги имаме потребните резултати:

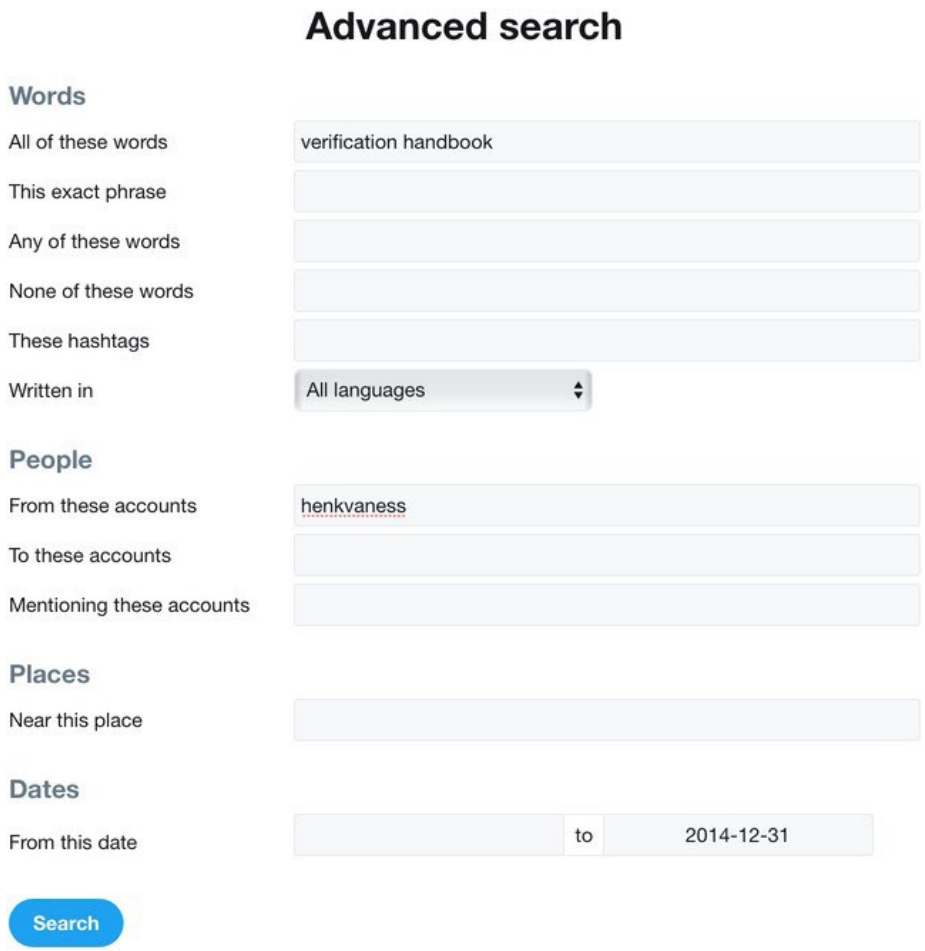


Твитер (Twitter)

Иако операторот за пребарување „site:“ има голема моќ, ќе бидете разочарани ако го користите на Гугл за да пребарате нешто во Твитер. На пример, можеме да пробаме со следната линија за да пронајдеме кога сум го поставил првиот твит за Прирачникот за верификација:

"verification handbook" site:twitter.com/henkvaness

Но, барем до моментов кога ги пишувам овие редови, враќа само еден резултат. Генеричките пребарувачи како што е Гугл често имаат тешкотии да обезбедат квалитетни резултати од илјадниците милијарди постови на Твитер, или на големите платформи како Фејсбук или Инстаграм. Одговорот, кога се работи за Твитер, е да се користат функционалноста за напредно пребарување (Advanced Search) со додавање на клучни зборови, корисничко име и временски период, како што е прикажано на следната слика:



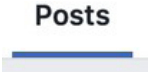
Не заборавајте да кликнете на копчето „Latest“ (Најново) на менито на врвот од страната со резултатите за да ви бидат прикажани во обратен хронолошки редослед. Автоматските поставки на Твитер се да ги подредува резултатите така што на врвот се твитовите за кои платформата смета дека се најдобри.

Фејсбук

Ниту на Фејсбук користењето на операторот „site:“ не е идеално. Од друга страна, можеме да ја прилагодиме неговата алатка за пребарување да одговори на нашите потреби. На пример, да речеме дека сакате да ги видите постовите за колач со јагоди што луѓето од Бруклин (Brooklyn) ги поставиле во март 2019 година. Следете ги следните чекори:

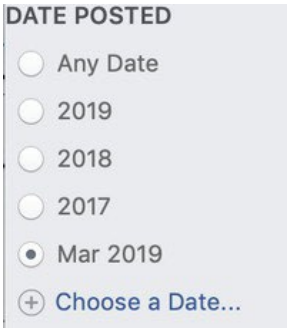
Чекор 1: Внесете ја фразата за пребарување

Чекор 2: Кликнете на постовите

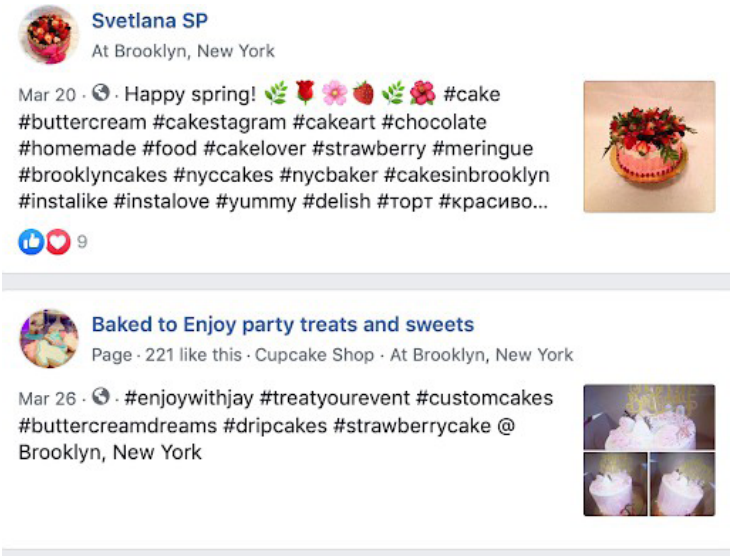


Чекор 3: Дефинирајте ја локацијата

Чекор 4: Изберете датум



Еве го резултатот:



Инстаграм

За пребарување на Инстаграм за постови од одреден датум на одредена локација, можете да ја посетите мојата веб-страница, whopostedwhat.com, и да го внесете вашето барање:

Instagram - Posts on Date Tagged With Location

Displays Instagram posts at a location on a certain date or earlier. Instagram will first show you a section called "Top Posts" containing a few rows of photos generated from an algorithm. The posts by date are in the section just below, named "Most Recent", where photos are sorted chronologically, newest first. Location URL looks like: https://www.instagram.com/explore/locations/95099702/mgm-grand-las-vegas/

Posts at Instagram location URL on Search

Example: *Find all posts from Las Vegas on July 4, 2019*

3. Препознавање на ботови, киборзи и неавтентични активности

Автори: Џоана Вајлд, Шарлот Годарт

Шарлот Годарт *(Charlotte Godart) е истражувач и обучувач во „Белингкет" (Bellingcat). Пред да се приклучи на Белингкет, работеш во Центарот за човекови права на Универзитетот на Калифорнија во Беркли (Human Rights Center at UC Berkeley), во тамошната Истражувачка лабораторија (Investigations Lab), каде ги обучуваше студентите како да вршат истражување на глобалните конфликти за меѓународните хуманитарни организации со користење на отворени извори.*

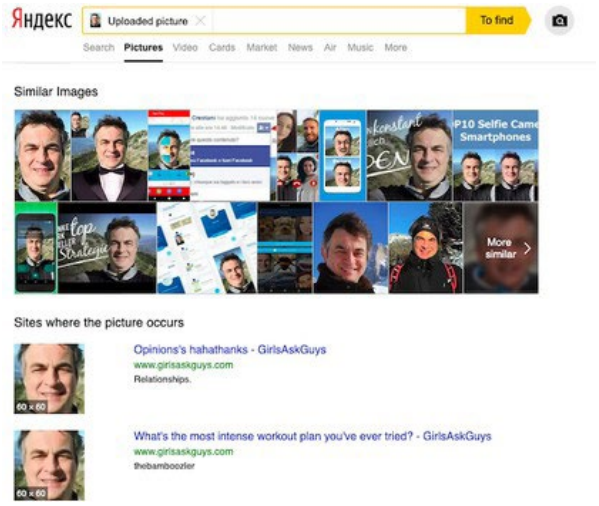
Џоана Вајлд *(Johanna Wild) е истражувач на отворени извори во „Белингкет" и е фокусирана на развој на технологии и алатки за дигитални истражувања. Има богато искуство во онлајн новинарството, а пред тоа има работено со новинари во (пост)конфликтни региони. Една од нејзините улоги беше да дава поддршка на новинари од Источна Африка во производството на емисии за „Гласот на Америка" (Voice of America).*

Кон крајот на август 2019 година, Бенџамин Стрик (Benjamin Strick), соработник на Белингкет и истражувач во „Окото на Африка" на БиБиСи (BBC Africa EYE), ги анализираше твитовите што ги шириа „хаштаговите" #WestPapua и #FreeWestPapua, кога забележа абнормално однесување на некои кориснички сметки. Тие кориснички сметки шириа про-владини пораки од Индонезија во момент кога конфликтот во Западна Папуа добиваше меѓународна видливост: Едно локално движење за независност излезе на улица во борбата за слобода од индонезиска контрола, што доведе до насилство помеѓу индонезиската полиција и демонстрантите.

Корисничките сметки што ги забележа Стрик покажуваа повеќе чудни сличности. Наскоро тој ќе сфати дека се работи за рани показатели за координирано неавтентично однесување. Но тој прво ги забележа ситниците.

Како прво, многу од сметките користеа украдени профилни слики. На пример, ја имате оваа сметка што наводно му припаѓа на лице што се вика Марко:

Со користење на алатката на Јандекс за реверзибилно пребарување на слики (Yandex's reverse image search tool), Стрик откри дека профилната слика на сметката претходно била користена на други веб-страници, со различни имиња. Ниту една од сметките што ја користеле фотографијата не припаѓала на вистинско лице со име „Марко“. Тоа потврдило дека сметките, во најмала рака, не ја говорат вистината за нивните вистински идентитети.



Освен лажните идентитети, Стрик исто така откри дека сметките објавуваат слична или дури идентична содржина и често меѓусебно се ретвитуваат. Уште повидливо беше дека некои од нив укажуваат на прецизна синхронизација и дека во временските кодови на нивните твитови се исцртуваат одредени урнеци. На пример, @bellanow1 и @kevinma40204275 најчесто ги објавуваа своите твитови во 7-та или 32-та минута на одреден час.

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

Мала е веројатноста човек да усвои таков ритам на твитување. Таквата синхронизација помеѓу повеќе сметки, комбинирана со лажните фотографии, сугерираше дека сметките не се поврзани со вистински идентитети и можеби се автоматизирани. Со анализа на сомнителните урнеци на однесување на сметките, Стрик конечно заклучи дека сметките се дел од про-индонезиска мрежа на „ботови“ на Твитер што шири едностран и заведувачки информации за судирот во Западна Папуа. (Повеќе за поголемата мрежа од која овие сметки беа дел можете да прочитате во студијата на случај 11б од овој Прирачник, „Истражување на информативна операција во Западна Папуа“.)

Што е „бот"? Одговорот е многу покомплициран од што би можеле да помислите

Случајот на Западна Папуа е далеку од единствената информативна операција што користи ботови на социјалните медиуми. Други операции се далеку попознати и покритикувани, иако во својата с'рж, сите сите имаат сличности во начинот на кој функционираат.

„Бот" е софтверска апликација што автоматски ги извршува задачите што и се доделени од луѓе. Дали ботот ќе прави добри или лоши работи во целост зависи од намерите на неговиот „сопственик".

Ботовите кои најчесто се спомнуваат во јавните дебати се социјалните ботови, активни на социјалните мрежи, вклучително и на Фејсбук, Твитер и ЛинкдИн (LinkedIn). На тие платформи, тие можат да се искористат за ширење на одредени идеолошки пораки, често со цел да се создаде впечаток дека постои голема поддршка на теренот за одредена тема, личност, содржина или „хаштаг".

Ботовите на социјалните медиуми главно влегуваат во три основни категории: ботови со временски распоред, ботови стражари и ботови засилувачи. Од големо значење е да знаете за каков бот се работи, затоа што секој од трите видови си има свои специфични цели и намена. Со секоја намена оди соодветен јазик и начин на комуницирање. Во контекст на дезинформациите, најмногу не интересираат ботовите за засилување на пораките.

Ботовите за засилување функционираат сосема во согласност со нивното име: засилуваат и шират содржина, со цел да влијаат и да го креираат јавното мислење на интернет. Можат да се користат и за создавање впечаток дека некои индивидуи или организации имаат многу повеќе следбеници од што реално е случај. Нивната моќ произлегува од бројноста. Мрежа од ботови за засилување може да се обиде да влијае врз „хаштагови", да шири линкови или визуелна содржина, или да оркестрира масовно спамирање или вознемирување на интернет, во обид да го дискредитираат лицето, да направат неговите ставови да изгледаат контроверзни или да изгледа дека се наоѓа во „опсадна" состојба.

Заедничкото дејство на многубројни ботови за засилување прави да изгледаат полегитимни, а со тоа да можат да го обликуваат пејсажот на јавното мислење на интерент. Ботовите за засилување што шират дезинформации тоа главно го прават преку „хаштаг-кампањи" или преку споделување вести во форма на линкови, видеа, „мимови", фотографии и други видови содржини. „Хаштаг-кампањите" вклучуваат ботови што постојано и координирано го твитуваат истиот хаштаг или група хаштагови. Целта често е да се измами алгоритамот за „трендирање" на Твитер за да додаде одреден хаштаг на листата на трендовски теми. Пример за такво однесување а „#Hillarysick", нашироко промовиран од ботови откако Хилари Клинтон (Hillary Clinton) се сопна на сцена во септември 2016 година, малку пред претседателските избори. (Значајно е да се забележи дека на хаштаг-кампањите ботовите не им се нужни и можат да постигнат поголем ефект без нивно користење. Погледнете го, на пример, ова истражување на Dawn за човечките „хаштаг фабрики" во Пакистан).

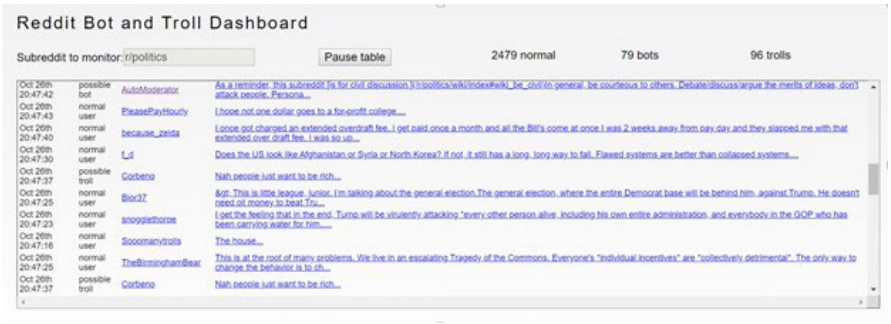
Купувањето и создавањето на ботови е релативно лесно. Недоброени веб-страници ќе ви ги продадат своите армии од ботови за неколку стотици долари или помалку. Од друга страна, многу потешко се создава и одржува мрежа од ботови што изгледа и се однесува како да се вистински луѓе.

Како да ги препознаете ботовите

Девелоперите и истражувачите создадоа многу алатки како помош во проценката дали некоја корисничка сметка е автоматизирана или не. Тие алатки можат да бидат корисни при собирањето информации, но наодите од една алатка ни од далеку не се дефинитивни и никогаш не смеат да бидат прифатени како единствена основа за известување или за носење заклучоци.

Една од најпознатите такви алатки е „Ботометар“ (Botometer), создадена од истражувачите на Универзитетот на Индијана. Врз основа на повеќе различни критериуми, тој пресметува поени за тоа колкава е веројатноста некоја корисничка сметка и нејзините следбеници да се ботови.

За Редит (Reddit), Џејсон Сковронски (Jason Skowronski) создаде командна табла што работи во реално време. Откако ќе ја прилагодите да ја следи избраната сметка на Редит (subreddit), таа се обидува да процени дали коментарите ги даваат ботови, тролови или вистински луѓе.



Иако има исклучоци, најголем број на јавно достапни алатки за детекција на ботови се создадени за Твитер. Причината за тоа е што многу социјални мрежи - вклучувајќи го и Фејсбук - имаат поставени ограничувања на АПИ (application programming interface, апликациски програмски интерфејс) што оневозможуваат јавноста да ги анализира и да ги користи нивните податоци за создавање на такви јавно достапни алатки.

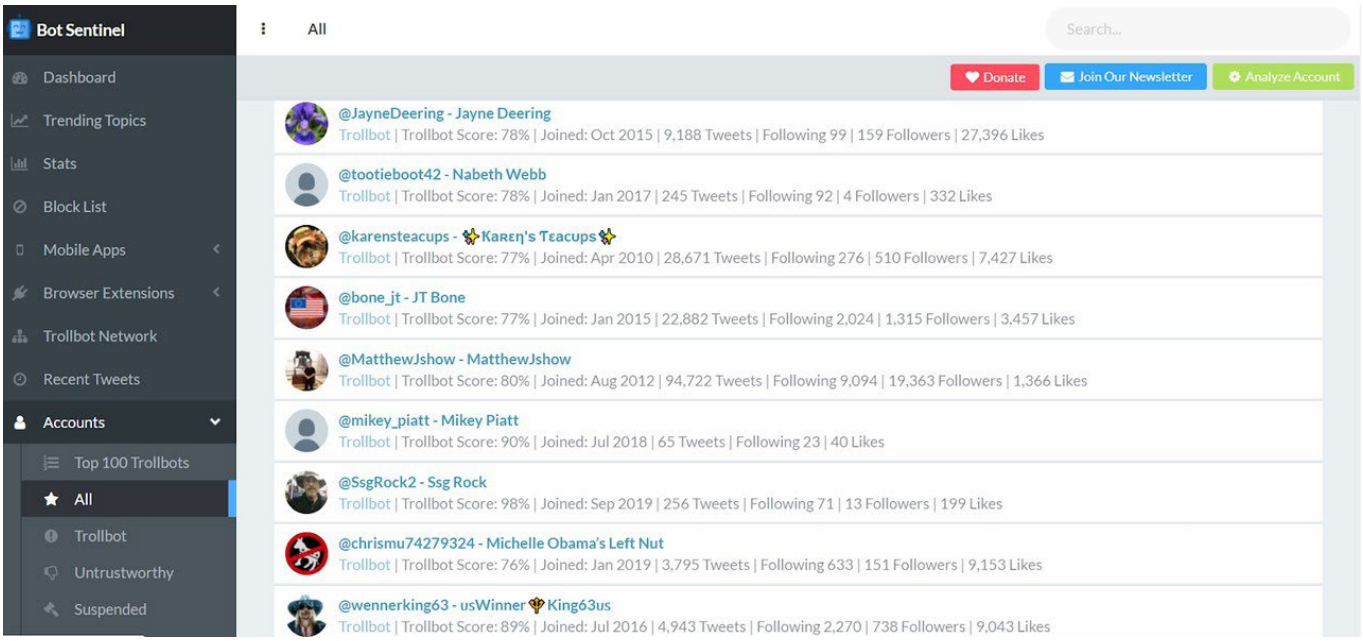
Како што веќе посочивме, алатките за детекција на ботови се добра почетна точка, но не треба да ви служат како единствен доказ. Една од причините за разликите во степенот на точност на нивните наоди е што едноставно не постои универзална листа на критериуми за препознавање на ботови што нуди стоотстотна сигурност во резултатите. Исто така, постојат разлики во ставовите дали нешто треба да се класифицира како бот. Истражувачите од Проектот за компутациска пропаганда на Оксфордскиот институт за интернет (Computational Propaganda Project, Oxford Internet Institute) ги класифицираат корисничките сметки што постираат повеќе од 50 пати на ден како „мошне автоматизирани“. Лабораторијата за дигитални форензички истражувања на Атлантскиот совет (the Atlantic Council’s Digital Forensics Research Lab) смета дека „72 твитови дневно (по еден твит на секои десет минути во период од 12 часа без одмор) се сомнителни, а повеќе од 144 твитови дневно се мошне сомнителни“.

Често е тешко да се утврди дали некоја кампања за дезинформирање ја водат социјални ботови или вистински луѓе мотивирани или платени да пострaвуваат големи количества содржини на одредена тема. На пример, БиБиСи откри дека корисничките сметки што поставуваа слични пораки на Фејсбук за засилување на содржини поволни за Борис Џонсон (Boris Johnson) во ноември 2019 година беа водени од луѓе што се преправале дека се социјални ботови.

Можете да наидете и на „киборзи“, сметки на социјалните мрежи што делумно се автоматизирани, а делумно со нив управуваат вистински луѓе, и на кои можете да најдете комбинација од природно и неавтентично однесување. Новинарите треба да избегнуваат да ги означуваат сомнителните кориснички сметки како ботови без доволно докази и соодветна анализа, затоа што погрешно обвинување може да го подрие вашиот кредибилитет.

Еден начин за справување со различните видови на ботови, киборзи и хиперактивни сметки водени од вистински луѓе е да го фокусирате истражувањето на следење на неавтентичното или однесување кое личи на автоматизирано, наместо да се обидете да идентификувате само еден вид на сомнителна сметка.

На пример, „Бот Сентинел“ (Bot Sentinel) нуди јавно достапна база на податоци на сметки на Твитер (од САД) со сомнително однесување. Креаторите на „Бот Сентинел“ одлучиле да ги соберат на едно место „сметките што постојано ги кршат правилата на Твитер“ наместо да се фокусираат на барање социјални ботови.



Чекори за истражување на неавтентично однесување

Генерално, го посочуваме следниот приод за идентификација на неавтентично и потенцијално автоматизирано однесување на социјалните мрежи:

1. Извршете „рачна“ проверка дали на сметките се јавува сомнително однесување.

2. Комбинирајте ја рачната проверка со користење на алатки или техничка мрежна анализа.

3. Истражете ги нивните активности, содржина и мрежата на други сметки со кои одржуваат контакти. Комбинирајте го претходното со традиционалните истражувачки техники, како што се обидите да ги контактирате нив или луѓето за кои тврдат дека ги познаваат.

4. Консултирајте надворешни експерти специјализирани за ботови и неавтентични активности.

За да откриете како рачно да им пристапите на сомнителните сметки, треба да ги знаете типичните знаци за предупредување за автоматизирани сметки на Твитер или на другите социјални мрежи.

На секој бот на социјалните медиуми му е потребен идентитет. Креаторите на ботовите сакаат нивните сметки да изгледаат што е можно поубедливо, а потребно е време за да се постават и одржуваат профили што изгледаат кредибилно, особено ако крајната цел е да се управува со голема мрежа на ботови. Колку повеќе сметки поседува некој, толку повеќе време одзема нивното создавање и управување на начин што ќе направи да изгледаат автентично. И токму тука таквите сметки прават грешки. Многу често се случува нивните креатори да вложат минимален напор да воспостават некој профил, и добар истражувачот може да го препознае тоа.

Еве неколку совети што да барате:

Нема вистинска профилна слика

Украдена профилна слика (како што откри истрагата на Бенџамин Стрик во Западна Папуа) или воопшто немање профилна слика може да биде индикатор за неавтентичност. Бидејќи креаторите на ботови сакаат да создадат многу сметки одеднаш, мораат да соберат колекција фотографии и често ги копираат од други веб-страници. Тоа, пак, создава неконзистентности. На пример, корисничка сметка со профилна слика од маж и корисничко име што сугерира дека жена е сопственичка на сметката може да сигнализира дека нешто не е во ред. За да го избегнат тој проблем, многу креатори на ботови бираат за профилна слика цртежи или слики од животни. Повторно, таа тактика станува нов урнек на однесување што може да се искористи за откривање на неавтентични сметки или сметки управувани од ботови.

Автоматско креирање на кориснички имиња

Следно, прегледајте ги имињата и корисничките имиња. Секој „прекар“ на Твитер е единствен и уникатен, што значи дека корисничкото име што го сакате често веќе е зафатено. За просечен човек тоа може да е мала незгода, но станува вистински предизвик и проблем ако се обидувате да креирате 50, 500 или 5,000 кориснички сметки во краток временски период.

Креаторите на ботови често користат стратегија што им помага полесно да пронајдат слободни кориснички имиња. За креирање на кориснички имиња се користат скрипти со критериуми како што се следниве:

Корисничко име следено од 4-цифрен број	12 карактери по случаен избор составена од големи или мали букви од (a-z, A-Z или бројки од 0-9)	Некое лично име следено од осум-цифрен број по случаен избор, што укажува дека се користи автоматски генерираното корисничко име од Твитер.
superman_1230	vP1tfl1ZoPG1	Neil03121977
superman_2313	dNi29j@utANQ	Sarah92839820
superman_9832	YQBrodhbPC84	Claire02938593
superman_3934	TUq3R6GBWYyA	John09340293
superman_4920	XI87NreGshx8	Stephen83749284

Ако забележите неколку сметки на Твитер со прекари што содржат ист број на букви и бројки, можете рачно да побарате повеќе сметки што го следат истиот урнек на листата на следбеници на таа сметка и потенцијално да идентификувате мрежа.

Во нашиот пример, сметките имаат нешто друго што им е заедничко: Сите се креирани во септември 2019 година. Во комбинација со други знаци, тоа може да биде индикатор дека сите сметки се подготвени во исто време, од истото лице.

Активностите на сметката не одговараат на периодот на нејзино постоење

Треба да бидете уште повеќе сомничави ако некоја нова сметка веќе има релативно голем број следбеници или ако објавила голем број на твитови во краток временски период. Истото се однесува и на постари сметки со многу малку следбеници, и покрај тоа што се многу активни.

Ако наидете на таква корисничка сметка, направете подлабока анализа на интензитетот на твитување. Земете го бројот на твитови наведен на врвот на страната и поделете го со бројот на деновите што поминале од моментот на активирање на сметката. На пример, имаме сметка што на 11 ноември 2019 година имала 3,489 твитови, а отворена е на 15 август 2019 година. Поделете 3,489 со 89 (бројот на денови од нејзиното активирање) и резултатот е 39,2 твитови дневно.

Дали бројот на твитови од моментот на активирање на сметката изгледа преголем, нереален или неодржлив?

Сомнителни обрасци на твитување

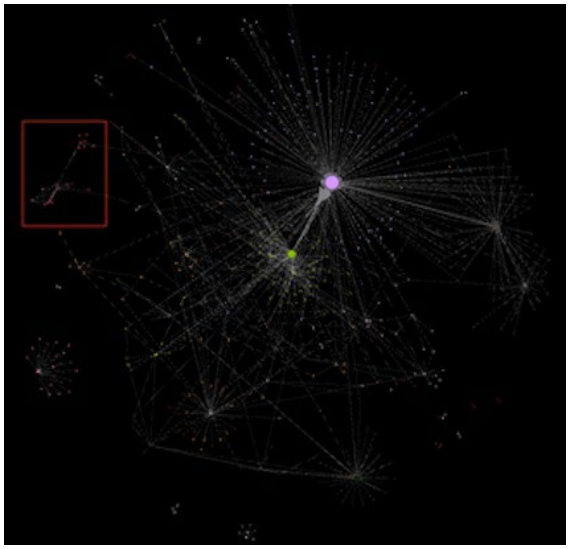
Друг елемент што треба да се провери е ритамот на твитување. Луѓето можат да имаат одредени преференци во смисла на тоа во кои денови или во кој период од денот твитуваат, но малку е веројатно некој да поставува твиоти само во понеделник, вторник и среда и целосно да е отсутен другите денови од неделата или во подолг временски период.

Ако сакате да ги забележите таквите шеми визуализирани за една одредена сметка, пробајте ја алатката за анализа на сметки развиена од Лука Хамер (Luca Hammer):

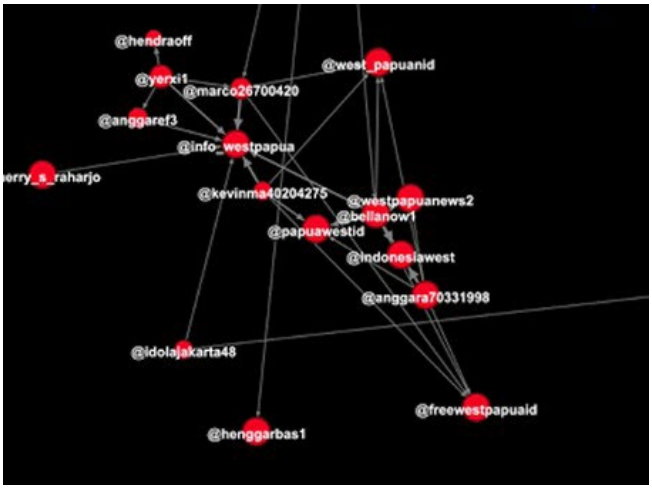
Визуализацијата како дел од истрагата

За подобро разирање на активноста на цела мрежа од ботови, можете да користите некоја од платформите за визуализација како што е „Гефи“ (Gephi). Соработникот на „Белингкет“ Бенџамин Стрик ја користеше оваа алатка за анализа на врските помеѓу корисничките сметки на Твитер што и припаѓаа на една про-индонезиска мрежа на ботови.

Со преглед на визуелната претстава на врските помеѓу голем број на сметки на Твитер, тој забележа дека отскокнува структурата на левата страна на сликата (означена со црвена боја).



Со зумирање, можеше да види кои сметки на Твитер се дел од таа специфична структура.



Секој црвен круг претставува една сметка а линиите ги претставуваат односите помеѓу нив. Вообичаено, повеќе мали сметки се распоредени околу голем круг во средината, што значи дека сите се во некаков однос со влијателната сметка. Сепак, сметките во структурата прикажана погоре немаат таков тип на интеракции една со друга. Тоа го поттикна Стрик да го анализира однесувањето на тие абнормални сметки.

Иднината на социјалните ботови: Дали можеме да ги надмудриме?

Технологијата што ги поддржува социјалните ботови многу напредуваше последниве години, овозможувајќи им на тие мали софтверски апликации да бидат многу повешти во симулирањето на човечко однесување. Веќе сме во точката во која луѓето предвидуваат дека вештачките корисници можат да влезат во софистицирана комуникација на интернет без нивните соговорници да забележат дека всушност влегле во долга конверзација со бот.

Сепак, до овој момент нема цврсти докази за постоењето и функционирањето на високо развиени социјални ботови што ја користат методата на машинско учење. За сега, изгледа дека повеќето кампањи за дезинформации се поддржани од помалку комплексни ботови за засилување.

„Не мислам дека има толку многу софистицирани социјални ботови што можат да водат вистински разговор со луѓе и да ги придобијат за одредена политичка позиција“, вели Др. Оле Пуц (Dr. Ole Pütz), истражувач во проектот „Непристрасни ботови што градат мостови“ (Unbiased Bots that Build Bridges) на Универзитетот Билефелд во Германија (University of Bielefeld).

Според него, најдобар начин да и се помогне на јавноста да го препознае неавтентичното однесување на социјалните мрежи е да користи метод на детекција што ги каталогизира и споредува сите фактори што ја прават една сметка сомнителна. На пример, тој вели, „Оваа сметка користи скрипта за ретвитирање на вести, автоматски ги следи другите сметки, а онаа друга сметка никогаш не користи урнеци на изразување што луѓето нормално би ги користеле“.

За сега, методичната анализа на однесувањето, содржината, интеракциите и мострите на однесување на сметката останува најдобриот начин за идентификација на неавтентично однесување.

Во делот за студија на случај, нудиме подетално техничко објаснување како ги анализиравме различните фактори во една сомнителна мрежа на Твитер, поврзана со протестите во Хонгконг.

за. Студија на случај: Пронаоѓање докази за автоматизирани активности на Твитер за време на протестите во Хонгконг

Автори: Шарлот Годарт, Џоана Вајлд Charlotte Godart, Johanna Wild

Шарлот Годарт *(Charlotte Godart) е истражувач и обучувач во „Белингкет" (Bellingcat). Пред да се приклучи на Белингкет, работеше во Центарот за човекови права на Универзитетот на Калифорнија во Беркли (Human Rights Center at UC Berkeley), во тамошната Истражувачка лабораторија (Investigations Lab), каде ги обучуваше студентите како да вршат истражување на глобалните конфликти за меѓународните хуманитарни организации со користење на отворени извори.*

Јохана Вајлд *(Johanna Wild) е истражувач на отворени извори во „Белингкет" и е фокусирана на развој на технологии и алатки за дигитални истражувања. Има претходно искуство во онлајн новинарството, а пред тоа има работено со новинари во (пост)конфликтни региони. Една од нејзините улоги беше да дава поддршка на новинари од Источна Африка во производството на емисии за „Гласот на Америка" (Voice of America).*

Во август 2019 година, Твитер го најави отстранувањето на илјадници кориснички сметки за кои тврше дека шират дезинформации за протестите во Хонгконг и се дел од „координирана операција поддржана од државата". Наскоро потоа, Фејсбук и Јутјуб објавија дека и тие отстраниле кориснички сметки што се дел од координирано неавтентично однесување во врска со протестите.

За разлика од Фејсбук и Јутјуб, Твитер објави и листа на отстранетите сметки, нудејќи можност за дополнително истражување на нивните активности. Со еден учесник на работилница организирана од Белингкет, нашиот тим одлучи да ги истражи преостанатите содржини за протестите во Хонгконг на Твитер, за да се обиде да идентификува знаци за координирано неавтентично однесување.

Пронаоѓање на сомнителни активности

Почнавме со пребарување на релевантните „хаштагови" за протестите. Едноставно пребарување со клучните зборови „Hong Kong Riots" („Хонгконг немири") пронајде многу твитови, некои од нив со повеќе од еден хаштаг.

Сакавме да се фокусираме на про-кинеските сметки и содржини, затоа што за нив Твитер веќе утврди дека се вклучени во неавтентични активности. Пробавме со различно формулирани клучни зборови, на пример:

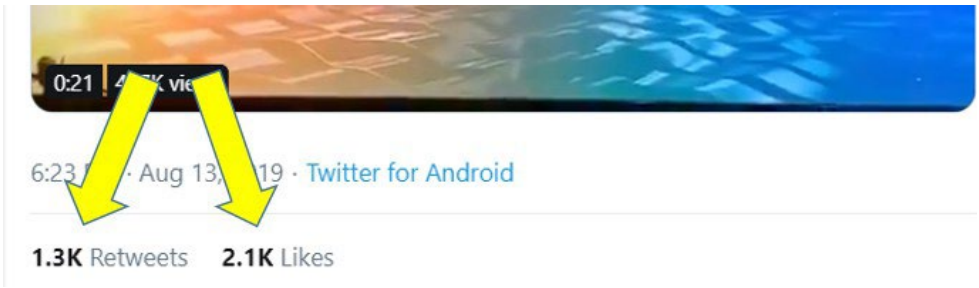
"Shame on Hong Kong" - police – government

Таквото пребарување дава резултати што ја содржат фразата „Shame on Hong Kong" („Срам за Хонгконг") но не и зборовите „police" (полиција) или „government" (влада). Целта беше да се филтрираат твитовите како што се „shame on hong kong police" („срам да ѝ е на полицијата на Хонгконг") и да се задржат твитовите како што е „shame on hong kong protesters" („срам да им е на демонстрантите во Хонг Конг"). Другите фрази за пребарување беа „Hong Kong roaches" („Лебарките од Хонгконг") и „Hong Kong mobs" („толпите од Хонгконг"), чести описи на демонстрантите на про-кинеските сметки на Твитер.

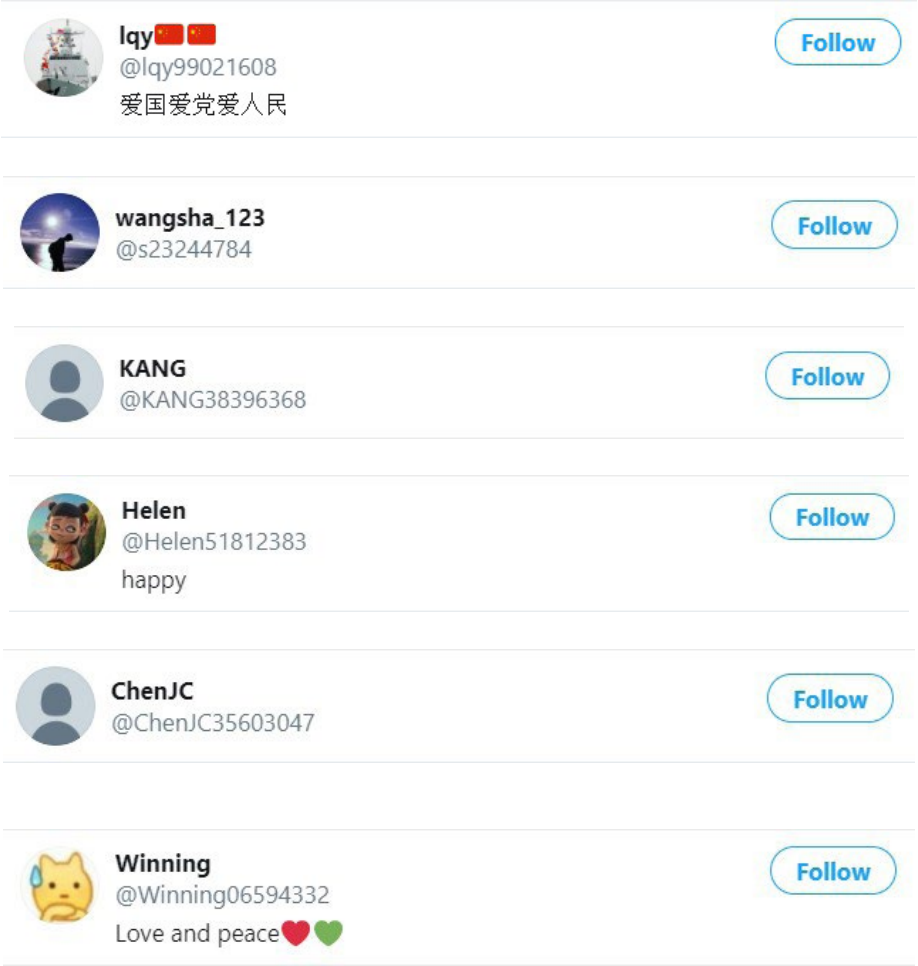
Откако извршивме пребарување со тие и други фрази, ги прегледавме скорешните твитови за Хонгконг што добија највеќе ретвитови и „допаѓања“. Резултатите можете да ги филтрирате според предизвиканиот ангажман со едноставно додавање на фразите “min_retweets:500” или “min_faves:500” кон фразата за пребарување. Така ќе ги добиете само твитовите со најмалку 500 ретвитови или „допаѓања“.

Потоа ги разгледавме сметките на Твитер што влегле во некаква интеракција со тие твитови. На пример, го имаме овој твит од верификуваниот корисник Ху Шиџин (Hu Xijin), главен уредник на кинеското и на англиското издание на „Глобал тајмс“ (The Global Times), кинески медиум во државна сопственост:

Кликнавме на линковите „Retweets“ (Ретвитови) и „Likes“ (Допаѓања) до секој број на ангажмани за да добиеме листа на сметките што го извршиле соодветното дејство.



Претпоставката беше дека неавтентичните про-кинески сметки ќе ги засилуваат твитовите на познатите личности што работат во кинеските државни медиуми. Во овој случај, отскокнуваат голем број на кориснички имиња затоа што имаа осумцифрен број по името, што посочуваше дека корисникот го прифатил корисничкото име што Твитер автоматски го генерира при отворањето на сметката. Тоа бараше дополнително истражување на нивното однесување и карактеристики.

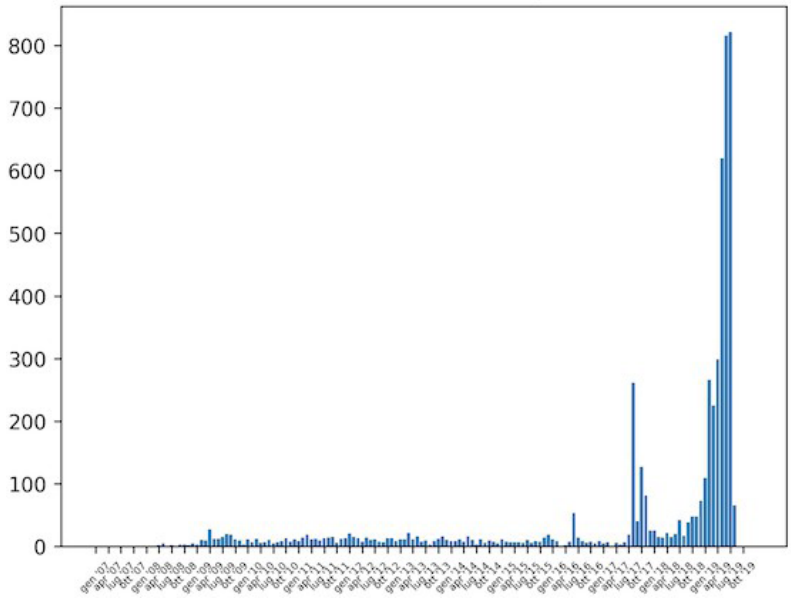


При прегледувањето на тие сметки, увидовме дека имаат многу малку следбеници, следат многу мал број сметки, нема биографии на сопствениците, ретвитуваат твитови од други луѓе и не поставуваат скоро ништо свое, и промовираат скоро исклучиво содржини што се против протестите.

Забележавме и дека тие сметки беа отворени малку порано, главно во август 2019 година. Бидејќи Твитер објави листа на отстранетите прокинески сметки, можевме да ги провериме датумите на регистрација на тие сметки и да видиме дали и тие го следат истиот тренд.

Со помош на Луиџи Губело (Luigi Gubello), програмер активен во задницата за отворени извори на интернет, искористивме едноставна скрипта напишана во програмскиот јазик „Пајтон“ (Python) (кодот можете да го пронајдете на неговата сметка на GitHub а повеќе информации за него имате овде) за да ги идентификуваме урнеците што се повторуваат во добиените податоци. Следниот графикон покажува дека сите отстранети сметки се отворени во претходните неколку месеци, во согласност со карактеристиките на активните сметки што беа предмет на нашето истражување.

Број на креирани сметки по месец



Автоматизација на процесот

Откако го идентификувавме примерокот на твитови со сомнителни карактеристики и однесување, сакавме да спроведеме многу подетална анализа. За тоа требаше да автоматизираме делови од процесот. Еден учесник на работилница на Белингкет имаше искуство во развој на софтвер, па напиша кратко парче код во програмскиот јазик „ЈавaСкрипт“ (JavaScript) - вообичаениот израз (\w+\d{8}) - за да изврши две функции: извлекување на корисничките имиња на сметките што ретвитувале или на кои им се допаднал одреден твит, и потоа брзо филтрирање на корисничкото име со фокус на корисничките имиња што следат ист образец. Образецот што го користевме за филтрирање беше лично име следено од број од осум цифри.

Со поставување на скриптата во конзолата за девелоперски алатки на „Хром“ (Chrome) што нуди алатки за веб-девелопери директно во пребарувачот, таа ќе се активира во позадина секогаш кога тој ќе кликне на линковите „Retweets“ (Ретвитови) или „Likes“ (Допаѓања) за одреден твит. Прикажаните резултати ќе ги посочат корисничките имиња што го следат тој образец. Овде можете да видите како изгледа тоа.

Сега можеме да ја користиме скриптата за да ги провериме сметките што влегле во интеракција со други познати про-кинески твитови. Среде протестите во Хонгконг, кинеско-американската актерка Лиу Јифеи (Liu Yifei) сподели пост на „Веибо“ (Weibo) со поддршка за полицијата, што водеше до тоа некои луѓе на социјалните мрежи да повикаат на бојкот на нејзиниот нов филм „Мулан“ (Mulan). Сепак, забележавме дека многу сметки на Твитер ја поддржуваа актерката и нејзиниот филм под хаштагот #SupportMulan. (СиЕнЕн, исто така, известуваше за ова прашање). Одлучивме да ја користиме скриптата за да ги провериме корисниците што ги ретвитувале или на кои им се допаднале твитовите за поддршка на Мулан.

Ги собравме имињата на сметките што се совпаѓаа со нашиот образец и ги идентификувавме датумите на кои се отворени. Откривме дека повеќето од нив се отворени на 16 август.

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

Податоците за точниот датум и време на регистрација на сметките ги собравме со едноставно преминување со глувчето преку информациите „joined“ (се приклучил) на профилот, како што е прикажано на следната слика:

Со сетовите од сметки пред нас, почнавме рачна анализа на содржините што ги споделувале. Набрзина стана јасно дека сите сметки на нашата листа твитувале во полза на Јифеи а против демонстрантите од Хонгконг.

Многу од сметките на нашата листа станаа неактивни после 17 или 18 август, што повторно укажува на постоење на координација. Не можеме точно да знаеме зашто преминаа во мирување, но можно е Твитер да побарал дополнителни чекори за верификација за сопствениците да можат да се најават, а тие не можеле да ги исполнат барањата. Втората опција е дека едноставно престанале да твитуваат затоа што нивните креатори не сакале да предизвикуваат натамошно сомневање откако Твитер почна да ги суспендира прокинеските сметки.

Неколку месеци подоцна, забележавме дека неколку од тие сметки повторно беа активни. По реактивирањето шириа позитивни пораки за Јифеи и нејзиниот филм „Мулан“.

Откривме и такви про-Мулан сметки со други обрасци на создавање на кориснички имиња и датуми на регистрација што континуирано шириа пораки во полза на Јифеи. Баравме твитови што вклучуваа специфични хаштагови, како што се #SupportMulan или #liuyifei


crystal_28cc @28ccCrystal · Aug 16
The real thugs are the demonstrators, not the police.
We support the leading artist of mulan and the Hong Kong police.#Mulan
#LiuYifei #supportmulan
4
18
168


MULAN
Follow
Mulan Our pride. ❤️
@kongyuting1
Liu Yifei is a good girl. ❤️He has Mulan's qualities of justice and courage and patriotism.❤️ He is our pride. ❤️Be happy. 刘包子。❤️
Joined August 2019
53 Following 65 Followers


Follow
Cinderlance·icc
@cinderlance
cuz u sucked some
Joined December 2017
48 Following 64 Followers


Mulan Our pride. ❤️ Retweeted
Choco @Choco_Xu · Aug 17
#SupportMulan #Mulan Democracy is not manifested by violence.Why can't people see the truth, she just stands on the side of justice?
Watch again
2:00 1.7K views
18
31
114

Cinderlance·icc Retweeted

Choco @Choco__Xu · Aug 17

#SupportMulan #Mulan Democracy is not manifested by violence.Why can't people see the truth, she just stands on the side of justice?

18 31 114

Mulan Our pride. ❤️ @kongyuting1 · Sep 25

#mulan #liuyifei #supportmulan #LiuYiFei #花木蘭 ❤️

> **十五小甜心** @SNH48_15 · Sep 22
>
> #liuyifei #Mulan Take you to know a real Liu Yifei (Mulan's actor). She always believes in one sentence, the harder she works, luckier she will be. I think one day, people will see the beauty of her bloom. twitlonger.com/show/n_1sr10p5

3

Cinderlance·icc @cinderlance · Nov 18

#liuyifei so sweet😘😘😘

6

Cinderlance·icc @cinderlance · Sep 18

#LiuYiFei 😘😘😘

Изгледа дека сметките ја промениле стратегијата од критикување на демонстрантите од Хонгконг на промоција на актерката и нејзиниот филм, можеби за да избегнат да бидат блокирани од Твитер.

Студијата на случај покажува дека е можно да се комбинираат рачни и автоматизирани техники за брзо откривање на мрежа на сомнителни сметки на Твитер. Таа, исто така, илустрира дека е корисно да се побараат дополнителни сметки и активности дури и откако платформата најавила дека ќе отстранува сметки.

Ние можевме да користиме неколку едноставни техники за пребарување и податоци за сметките за да идентификуваме поголем сет на сметки со видливи показатели дека се ангажирани во координирана неавтентична активност.

4. Мониторинг за откривање на лажни информации во периоди на ударни вести

Автор: Џејн Литвиненко

Џејн Литвиненко *(Jane Lytvynenko) е искусен репортер во БазФид Њуз (BuzzFeed News) фокусирана на прашањата на дезинформациите, кибер-безбедноста и онлајн истражувањата. Во својата работа има разоткриено кампањи за манипулација преку социјалните медиуми, измамници со крипто-валути и финансиски мотивирани злонамерни актери што шират дезинформации. Исто така, таа обезбедува пристапна проверка на факти за поширокатa публика во кризни ситуации. Џејн е од Киев, Украина, а во моментов живее во Торонто, Канада.*

Кога настануваат вестите, можат да поминат часови или дури денови пред известувачите и официјалните лица да можат целосно да разберат некоја состојба. Како што доказите и деталите почнуваат да течат по социјалните мрежи и други онлајн платформи, можат да се појават злонамерни актери што сакаат да шират поделби и недоверба, или набрзина да заработат од вниманието на загрижените потрошувачи на вести. Истите тие добронамерни потрошувачи и други извори можат и ненамерно да шират лажни или заведувачки информации. Смесата од повишени емоции и спориот тек на вести во првите минути и часови од некој настан повлекува потреба кај новинарите да бидат добро опремени за ефективно следење, верификација и - ако е потребно - раскринкување на ударни вести. Потребни се неколку минути да се креира лажен твит, слика, сметка на социјалните медиуми или статија, додека вистинските информации имаат проблем да држат чекор со таквата брзина.

Клучно за следењето и раскринкувањето кај ударните вести е да ги поставиме основите уште пред настанот да се случи. Тоа значи поседување на солидна основа во базичните вештини за верификација, како оние наведени во првиот „Прирачник за верификација“, разбирање како се следат социјалните мрежи и платформи, и знаење како да се одговори ако вие или вашите колеги станете цел на злонамерните актери. Репортерите никогаш не треба да ја запоставаат безбедноста во онлајн сферата.

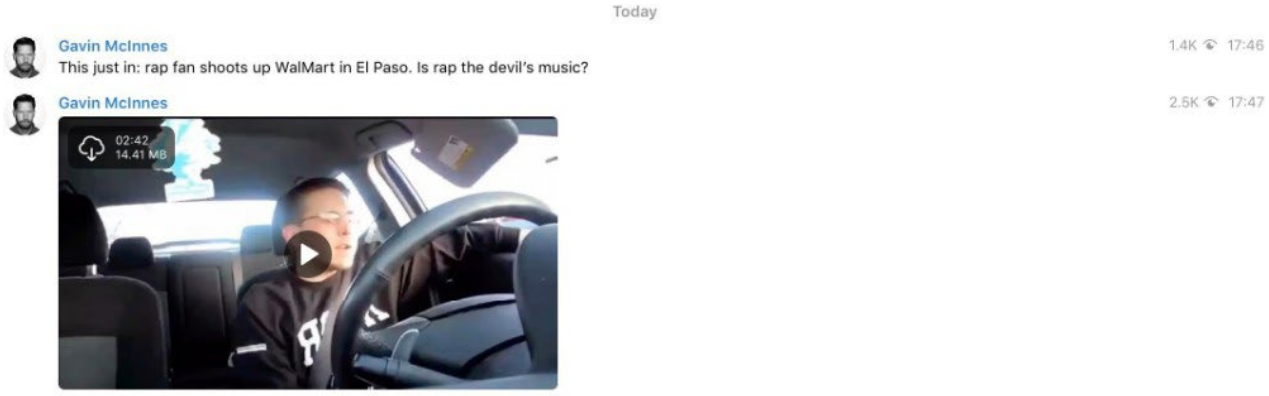
При настапувањето на ударни вести, првиот чекор е да се идентификуваат клучните засегнати заедници. Кога се случи нападот на средното училиште во Паркленд, Флорида (Parkland, Florida) во 2018 година, репортерите ја прочешлаа мапата на „Снепчет“ (Snapchat) барајќи видеа од тоа што се случува со учениците заробени во училниците. Од друга страна, за време на ураганот „Ирма“ во 2017 година, од клучно значење беше фокусот на Фејсбук, затоа што оние што беа под удар на невремето се обидуваа таму да ги пронајдат потребните информации. Од клучно значење е разбирањето како функционира секоја индивидуална социјална мрежа и како таа се пресекува со одреден настан.

Во ова поглавје се фокусираме на алатките што еден репортер може да ги користи за следење и раскринкување во случај на ударна вест. Не секоја алатка е соодветна за секоја ситуација, а разбирањето кој претрпел најголемо влијание од настанот може да ви помогне да утврдите каде да го насочите вашето внимание.

Три работи на кои треба да внимавате

Додека платформите и репортерите макотрпно се борат со дезинформациите, злонамерните актери ги развиваат своите тактики за избегнување на нивно откривање. Сепак, некои обрасци на однесување и содржини постојано се јавуваат.

1. **Обработени слики и слики дадени вон контекст.** Озлогласената слика на ајкула што плива по поплавен автопат секогаш повторно се јавува и продолжува да ги залажува луѓето со години. (Таа беше предмет на студија на случај објавена во првиот Прирачник.) Сликите и видеата што веќе биле раскринкани се она што проверувачите на факти и раскринкувачите го нарекуваа „зомби измама“ (zombie hoax) и треба да се внимава на нив. Сликите се шират по дигиталните платформи многу побрзо од текстот, па фокусот на нив често носи добри резултати.



За време на нападот со огнено оружје во „Волмарт“ (Walmart) во Ел Пасо, во 2019 година, претставници на крајната десница се обидоа погрешно да претстават едно старо видео објавено на Јутјуб, неповрзано со осомничениот на никаков начин.

2. **Лажни жртви или сторители.** За време на нападот со огнено оружје на централата на Јутјуб, социјалните мрежи беа преплавени со лажни дојави за осомничени сторители. За време на преодните Избори во САД во 2018 година, Претседателот на САД шириле лажни гласини дека нелегални имигранти гласале на изборите. Лажни сторители се јавуваат кај најголем број големи настани што претставуваат ударни вести.

За време на нападот со огнено оружје во Паркленд во 2018 година, лажна сметка на Бил О’Рајли (Bill O’Reilly) се обиде да прошири лажно име на осомничениот за пукањето.

3. **Вознемирување и координирани напади („бригадирање“).** Иако не се работи стриктно за дезинформација, злонамерните актери вообичаено се обидуваат да ги вознемируваат луѓето инволвирани во некој настан, во обид да ги замолчат. Тоа, исто така, е знак дека група луѓе се занимава со некој настан и може да проба да употреби различни тактики со текот на времето. За соработката на група луѓе за да создадат впечаток за голем и масовен ангажман или реакција се користи терминот „бригадирање“ (brigading). Пример е гласањето за или против одредена содржина или преплавување на некој корисник со коментари.

По дебатата на раководството на Демократите во 2019 година, анонимни сметки на социјалните медиуми ја шират истата порака за расната припадност на Камала Харис (Kamala Harris).

Најдобри практики на архивирање и објавување

Пред да почнете да барате измами, подгответе една папка за вашата документација и табела во која ќе ги внесувате наодите. Веднаш направете снимка од приказот на екранот (screenshot) од секоја измамничка или друга релевантна содржина што сте ја открите и архивирајте ја страната. (Додатокот за веб-прелистувачи The Archive.org е бесплатна, брза и ефективна алатка за архивирање на содржини.) Осигурајте се дека сте ги запишале и оригиналните и архивираните УРЛ адреси за откриената содржина во вашата табела. Тоа ќе ви овозможи да се навратите на тоа што сте го пронашле и да барате обрасци на однесување подоцна, откако ќе се слегне прашината.

За да избегнете и самите да ги ширите страниците поврзани со дезинформации или мисинформации, во сите статии или постови на социјалните медиуми поставувајте го линкот до архивираната а не до оригиналната УРЛ адреса. Друга добра практика е да поставите „воден жиг“ на вашите слики со јасна ознака како што е „Лажно“ (False) или „Заведувачко“ (Misleading) за да обезбедите дека ќе бидат ширени и индексирани во правилен контекст. Ако пишувате статија, во насловот и во текстот фокусирајте се на она што е вистина, наместо првенствено да кажувате што е лага. Минати студии и истражувања покажуваат дека повторувањето на лажните информации предизвикува луѓето да ги задржат погрешните информации.

Вашата улога е да го минимизирате повторувањето на лажните информации колку што е можно, и да ги водите луѓето кон точните информации.

Идентификување на клучните зборови и локации

Со текот на настаните, подгответе листа на локации и релевантни клучни зборови.

За листата на локации, земете ги предвид градот, округот, федералната единица или државата, како и сите релевантни локализми, како што е прекарот по кој се познати жителите на градот или на некој кварт или соседство. Ако се работи за избори, треба да ги заведете соодветниот округ или името на изборната единица. Таквите информации се користат за следење на географски означени (geotagged) постови и за пребарување на спомнувањата на дадената локација. Исто така, идентификувајте ги и почнете да ги следите сметките на социјалните мрежи на сите релевантни локални органи, како што се полицијата или против-пожарната служба, политичарите и локалните информативни медиуми.

Следно, идентификувајте ги клучните термини. Тука можат да влезат зборови како жртва, осомничен, стрелец, пукање, поплава, пожар, потврдените имиња на инволвираните лица, како и поопшто формулирани фрази како „се бара“ - размислете каков речник, освен клучните термини, би можеле луѓето да користат во соодветната ситуација. Ако пронајдете кредибилна сметка што постирала дека се наоѓа среде настанот што го следите, забележете го корисничкото име и прочитајте сè што постирала. Прегледот на нивните листи на следбеници и пријатели може да биде корисен начин да се пронајдат други луѓе во таа област што можеби трпат влијание од настанот.

Имајте на ум дека, во стресни ситуации, луѓето можат да направат грешка во пишувањето на имињата на локациите или личните имиња. На пример, за време на пожарот во Кинкејд, Калифорнија (Kincade, California) во 2019 година, некој твитувал со хаштаг #kinkaidfire поради проблеми со алатката за авто-корекција. Вклучете ги најчесто користените погрешно напишани имиња во вашето пребарување и обидете се да ги идентификувате можните грешки на авто-корекцијата со внесување клучни термини во вашиот уред за да видите какви сугестии ќе ви бидат понудени.

Тоа е добар момент да пробате да контактирате некои од изворите што ги знаете од соодветната локација, или кои се дел од заедници што можеби се цел на вознемирување или дезинформации, и прашајте ги што тие виделе дека кружи на интернет. Можете на вашата публика да и кажете дека барате дезинформации и други проблематични содржини поврзани со настанот. Координирајте ги активностите со тимот за социјални медиуми во вашата редакција за да разгласите дека ја следите ситуацијата и да видите дали публиката забележала нешто значајно.

Клучни алатки за работа со слики

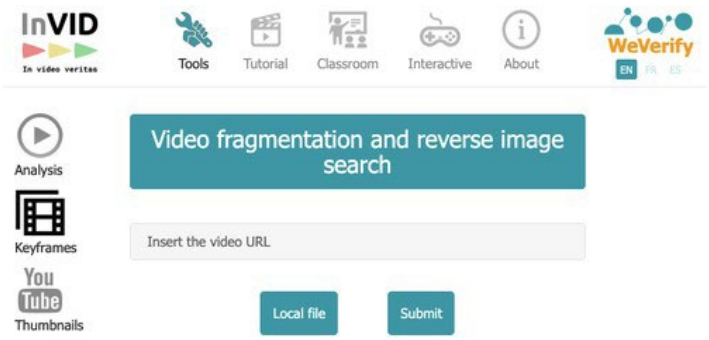
1. *Пребарување на слики*

Реверзибилното пребарување на слики е незаменлива алатка. Пребарувањето на слики на Гугл е едноставно и сè што е потребно е десен клик на сликата и избор на „Search Google for Image“ („пребарајте слика на Гугл“) на менито во веб-прелистувачот Хром (Chrome). Сепак, секогаш е добро да се пребара некоја слика со користење на различни алатки. Ако во вашиот прелистувач ја инсталирате екстензијата „ИнВИД“ (InVID), со десен клик на сликата можете да пребарате каде сè е објавена со повеќе алатки одеднаш. Следниот приказ на споредбено реверзибилно пребарување слики подготвено од „Домеин тулс“ (Domain Tools) ги покажува релевантните добри и лоши страни на различни сервиси за реверзибилно пребарување слики:

	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

ИнВид (InVID)

„ИнВИД“ (InVID) е бесплатна екстензија за веб-прелистувачи и најдобра платформа за анализа и верификација на видео содржини. Дозволува корисниците да внесат УРЛ адреса и нејзината машина потоа ќе направи слики (thumbnails) од индивидуални кадри од видеото. Тие слики потоа можете да им правите реверзибилно пребарување за да видите каде на друго место на интернет се појавило тоа видео.



2. *Пребарување „ТвитДек“ (TweetDeck)*

Најдобар начин за пребарување на Твитер е со користење на „ТвитДек“ (TweetDeck), алатка што овозможува креирање на единствени колони за пребарувања и листи.

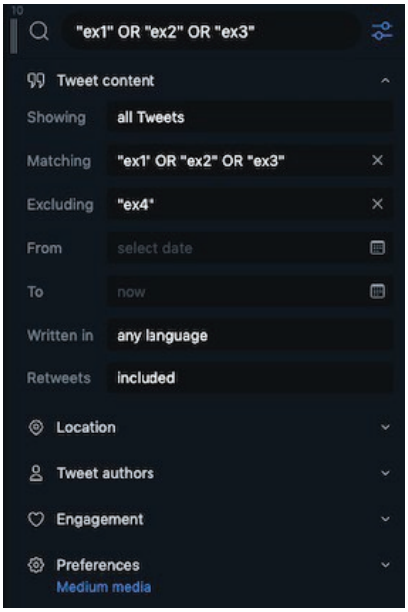
Наоѓањето и дуплирањето на релевантните листи е клучно за да се држи чекор со некоја ситуација. Листи на Твитер можете да пребарувате и на Гугл, со користење на едноставна формула. Внесете *site:twitter.com/*/lists* во пребарувачот и додадете го клучниот збор во наводници, на пример “Alabama reporters” (Репортери од Алабама). Значи, фразата за пребарување гласи:

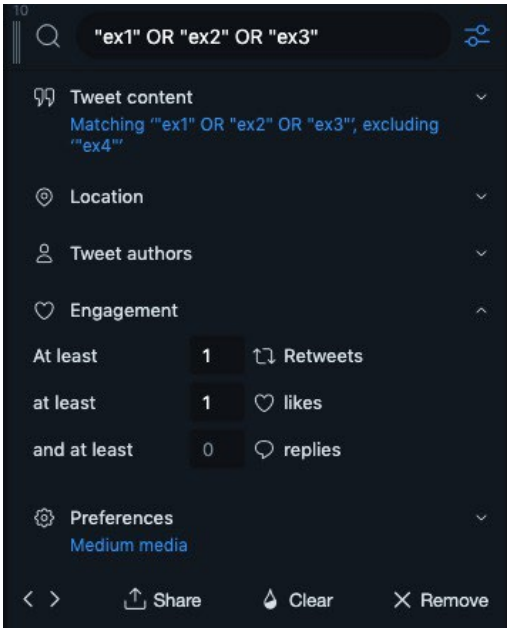
site:twitter.com//lists “Alabama reporters”*

Така ќе ги добиете сите листи креирани од други корисници на Твитер што ја вклучуваат фразата „Репортери од Алабама“ во насловот.

Кога ќе пронајдете листа што одговара на вашите потреби, треба да ја дуплирате за да можете да ја додадете во ТвитДек. Користете ја апликацијата: http://projects.noahliebman.net/listcopy/connect.php за дуплирање на онолку листи колку што сакате. Дуплирањето е подобро од следењето на листа, затоа што потоа можете да додавата или одземате корисници по потреба.

Паралелно со пронаоѓањето и додавањето листи во колоните на ТвитДек, треба да креирате колони со специфични филтри за пребарување што ќе ви овозможат брзо следење на клучните зборови, слики и видеа. За преглед на повеќе клучни зборови одеднаш, ставете ги во наводници и впишете „OR“ меѓу нив, на пример: „Kincade“ OR „Kinkade“. Можете и да исклучите одредени зборови ако произведуваат нерелевантни резултати. Повеќето луѓе не додаваат ознаки (tag) за локација на своите твитови, па тоа поле можете да го оставите празно за мрежата да ја фрлите пошироко.





Ако сакате да ги стесните резултатите, поставете го датумот во полето „From“ еден или два дена пред да се случи настанот, за да избегнете да испуштите некои твитови поради разликите во часовните зони. Ако сè уште добивата премногу резултати, обидете се да ги филтрирате преку бројот на ангажмани за на површина да излезат само твитовите што некој ги ретвитувал или му се допаднале. Можете да се обидете да ги одвоите клучните термини во посебни колони. На пример, внесете ги локациите во една колона а другите клучни зборови во друга. Јас обично правам трета колона за внесување на можните имиња на осомничените или на жртвите, како и варијантите за пишување на нивните имиња.

Конечно, ако излегуваат премногу твитови, добра идеја е да креирате нова колона со најдобрите клучни зборови, и да ја изберете опцијата „Showing“ под филтерот „Tweet content“ за да се прикажат само фотографии и видеа. Така ќе добиете листа на содржини што ќе помогне да ги забележите виралните или новите визуелни материјали.

3. *КраудТенгл (CrowdTangle)*

„КраудТенгл“ (CrowdTangle) е веб-апликација и додаток за прелистувачи што редакциите можат да го користат без надомест. (Контактирајте ја компанијата што ги произведува ако вашата редакција нема пристап.)

Се работи за моќна алатка што дозволува прилагодување на контролните панели за истовремено следење на Фејсбук, Инстаграм и Редит. Можете да пребарувате со клучни зборови и да поставите повеќе филтри, вклучително и времето на објавување, јазикот и предизвиканиот ангажман. „КраудТенгл“ е особено корисен за следење на Фејсбук и проверка каде на социјалните медиуми била поставена некоја УРЛ адреса.

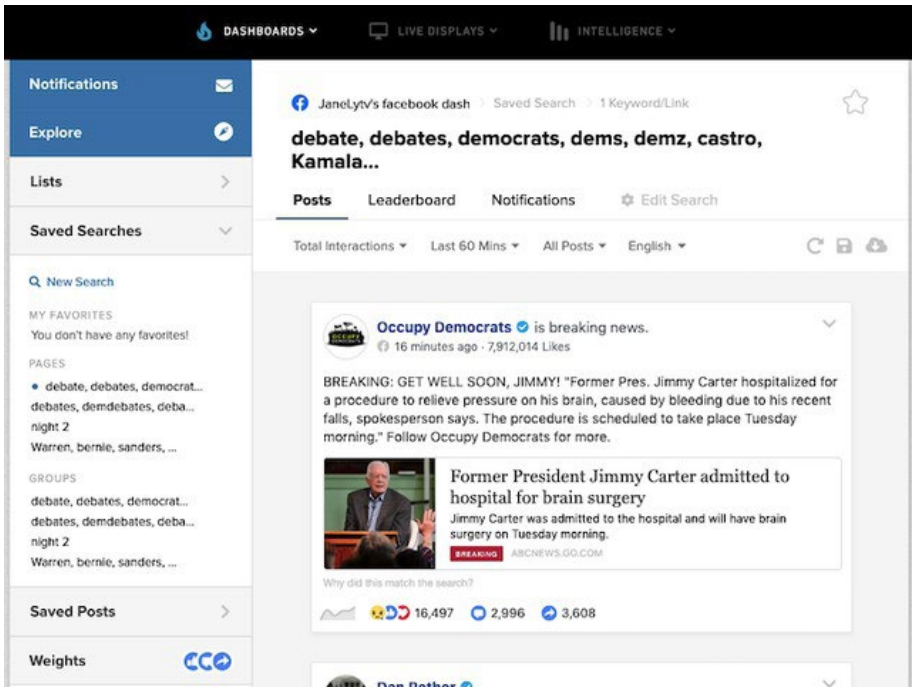
Кога ќе добиете пристап, преминете на app.crowdtangle.com и кликнете на „Create New Dashboard“ (Креирајте нова контролна табла). Дури и ако немате пристап, додатокот за прелистувачи е бесплатен за користење за сите.

КраудТенгл: Пребарување на постови на Фејсбук

Кликнете на „Saved Searches“ (Снимени пребарувања) на менито од левата страна, а потоа кликнете на „New Search“ (Ново пребарување). Кај Фејсбук имате две можности: да пребарувате страници или да пребарувате групи. Препорачувам да ги спроведете двете пребарувања. Внесете онолку клучни зборови колку што сакате, одвоени со запирки. Тогаш можете да го дефинирате начинот на прикажување на постовите, на пример, по старост, по популарност или по неочекувано голем успех, што е мерка за постовите што добиваат повеќе ангажман отколку што е нормално на соодветната страница. Јас преминувам од еден на друг начин, во зависност од ситуацијата, за да се осигурам дека ќе би забележам виралните и новите содржини.

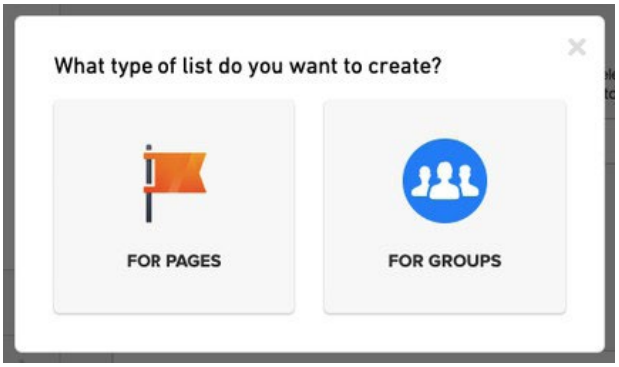
Можете да ги подредите постовите по специфична временска рамка или по тип. КраудТенгл неодамна додаде можност за пребарување на постовите по локација на страницата на која се поставени. Со клик на опцијата „English“ и избор на државата („Country“) можете, на пример, да ги изберете само постовите што доаѓаат од страници што јавно се изјасниле дека се лоцирани во САД. Можете да го сторите и спротивното и да барате постови што доаѓаат од страници лоцирани во Иран, Русија, Саудиска Арабија, Филипините или, на пример, Индија. Обрнете особено внимание на постовите во чија основа е некоја слика или видео, затоа што тие имаат тенденција да досегнат подалеку и да предизвикаат повеќе ангажман.

Откако сте го прилагодиле барањето за да добиете релевантни резултати, снимете го за да можете да му се навраќате кога е потребно.



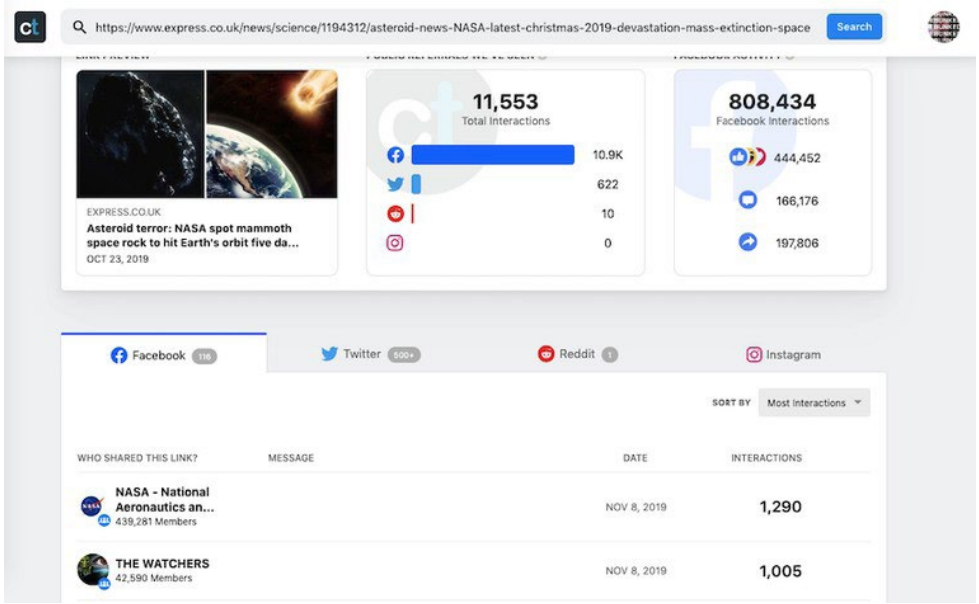
КраудТенгл: Листи

Како и „ТвитДек“, „КраудТенгл“ овозможува да подготвите листи на страниците и јавните групи што ве интересираат. Со клик на опцијата „Lists“ (Листи) на левото мени и избор на опцијата „Create List“ (Креирајте листа), можете да ги следите страниците или групите што се совпаѓаат со избраните клучни зборови или страниците чии УРЛ адреси ги имате. „КраудТенгл“ исто така нуди повеќе готови листи што можете да ги прегледате со клик на јазичето (tab) „Explore“. Како и кај Твитер, подготовката на листа страници или групи на кои се говори за настанот за кој известувате е добар начин да се следи информативната средина.



КраудТенгл: Пребарување на линкови

Друга релевантна функција на „КраудТенгл“ е пребарувањето на линкови (link search). Одете на https://apps.crowdtangle.com/search/ и внесете ја УРЛ адресата или клучните термини на содржината што ве интересира. „КраудТенгл“ ќе ви ги прикаже луѓето што најчесто го споделиле тој линк на Фејсбук, Инстаграм, Редит и Твитер. (Имајте на ум дека резултатите за Твитер се ограничени на претходните седум дена.) Тоа ќе ви помогне да разберете како се шири содржината, дали постојат групи или индивидуални лица што ќе треба дополнително да ги проверите и истражите, и дали содржината е доволно проширена за да треба да се направи нејзино раскринкување. Не постојат едноставни правила кога треба да се врши раскринкување на некоја невистина, но некои од прашањата што треба да си ги поставите се: Дали се проширила надвор од почетната мрежа на споделувачи? Дали ја споделувале лица што поседуваат одреден авторитет во јавноста? Дали предизвикала сериозен ангажман? (Бесплатниот додаток за прелистувачи ги дава истите податоци како и алатката за пребарување линкови. И двете се бесплатни за користење за сите без потреба да се поседува полна сметка на „КраудТенгл“.)

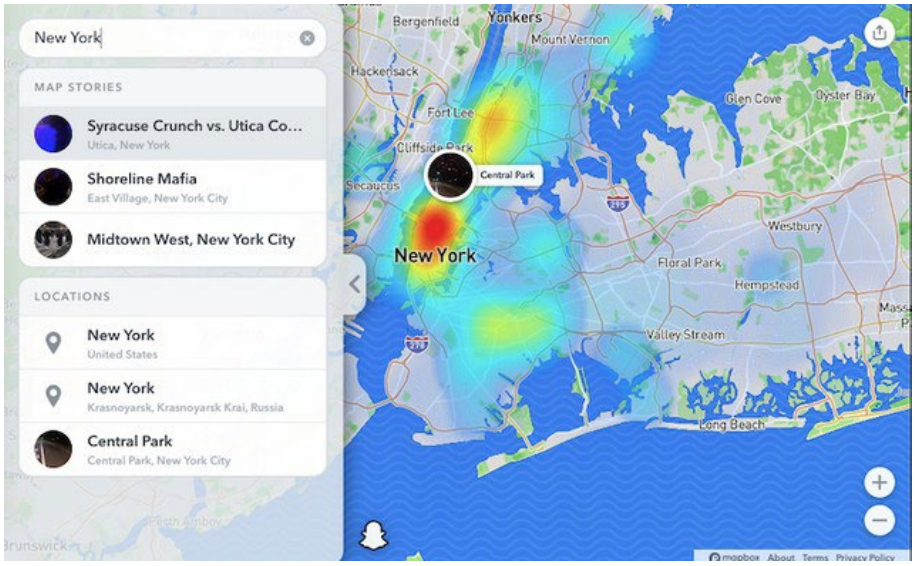


4. *Instagram.com*

Инстаграм е корисно место за следење на хаштагови и гео-тагирани постови. Побарајте ги релевантните локации на кои корисниците можеби означиле (тагирале) фотографии, и имајте на ум дека локациските ознаки вклучуваат и соседства и знаменитости. Откако ќе пронајдете некој кој изгледа дека бил вклучен во некој настан, посетете ја неговата корисничка сметка и задолжително прегледајте ги нивните приказни (stories) - тие се многу попопуларни од обичните постови на Инстаграм. Прегледајте и коментарите за да идентификувате други можни сведоци и нови хаштагови што можеби биле користени со нивните постови. Ако сакате да архивирате нечија Инстаграм приказна, приказната можете да ја снимите со користење на услугите на веб-страници како што е storysaver.net.

5. *СнепМеп (SnapMap)*

Дезинформациите не се честа или вообичаена појава на „Снепчет“ (Snapchat), но неговата функција на јавна географска карта е корисна во верификацијата или во раскринкувањето на измами. За почеток, појдете на map.snapchat.com и внесете ја локацијата што ве интересира. Ќе ви биде прикажана термална мапа на локациите на кои е поставена содржината - што посветла е бојата на локацијата, толку повеќе снеп-пораки (Snaps) потекнуваат од неа. За зачувување на корисен „Снеп“, кликнете на трите точки во горниот десен агол на екранот и изберете „Share“ (Сподели). Ќе можете да ја копирате УРЛ адресата на тој Снеп за да го прегледате подоцна. (Секако, задолжително направете и снимка од екранот (screenshot).)



Собирање сè заедно

Од клучно значење е да вежбате како се користи секоја од алатките пред да настапи некоја ударна вест за да избегнете ситуација во која ќе мора да се снаоѓате и да учите во од. Намената на дезинформацијата е да удира на емоциите и да ги користи празнините во медиумското известување. Бидете свесни за тоа кога пребарувате по интернет. Често ќе наидете на точни информации што можат да им помогнат на вашите колеги. Запишете сè за што знаете дека е вистина за да можете полесно да го препознаете она што е лажно, и не плашете се да побарате помош од кој било од репортерите од вашиот медиум што се наоѓаат на лице место.

Откако ќе слегне прашината, добро е да им се вратиме на снимените слики и постови. Иако во тој момент, како практичар на новинарството како јавен сервис, сакате да ги посочите индивидуалните лаги и лажни информации, подоцна треба да направите попис на сите видливи теми и обрасци. Дали луѓето станале цел на кампањата поради нивната расна или родова припадност? Дали измамите што прв пат се јавиле на мали, анонимни кориснички сметки влегле во мејнстримот? Дали некоја компанија што раководи со социјален медиум имала особено добра или особено лоша изведба? Една сумирана статија може да им помогне на вашите читатели целосно да ги разберат целта и методите на ширење на дезинформацијата. Статијата ќе послужи и како алатка за истражување и за вас и за вашата редакција преку укажување на кои нешта ќе треба да се фокусирате следниот пат кога ќе се случи ударна вест.

5. Верификација и проверка на слики и илустрации

Автори: Хана Гај, Фарида Вис, Сајмон Фокнер

Фарида Вис *(Farida Vis) е директорка на Лабораторијата за визуелни социјални медиуми (Visual Social Media Lab) и професорка по дигитални медиуми на Универзитетот „Манчестер Метрополитен" (Manchester Metropolitan University). Нејзиниот академски интерес и работата во областа на дата-новинарството се фокусирани на ширењето на погрешни информации на интернет. Таа беше членка на Советот за социјални медиуми на Глобалната агенда на Светскиот економски форум (World Economic Forum's Global Agenda Council on Social Media) од 2013 до 2016 година, како и на Советот на „Глобал Фјучер" за информации и забава (Global Future Council for Information and Entertainment) од 2016 до 2019 година, а во моментов ја врши должноста на директорка на „Опен дата Манчестер" (Open Data Manchester).*

Сајмон Фокнер *(Simon Faulkner) е предавач по историја на уметноста и визуелна култура на Универзитетот „Манчестер Метрополитен". Неговата истражувачка работа се занимава со политичката употреба на сликите и нивното значење, со особен фокус на активизмот и протестните движења. Тој е ко-директор на Лабораторијата за визуелни социјални медиуми (Visual Social Media Lab) со интерес во областа на развојот на методи за анализа на слики објавени на социјалните медиуми..*

Хана Гај *(Hannah Guy) е докторанд на Универзитетот „Манчестер Метрополитен", каде ја истражува улогата на сликите во ширењето на дезинформациите на социјалните медиуми. Таа е членка на Лабораторијата за визуелни социјални медиуми, а нејзините тековни проекти се однесуваат на сликите споделувани на Твитер во времето на појавата на движењето „И црните животи се важни" (Black Lives Matter), како и на писменоста за визуелните медиуми (Visual Media Literacy) во борба со дезинформациите во контекст на канадскиот образовен систем.*

Комуникацијата на социјалните медиуми денес е доминантно визуелна по природа. Фотографиите и видео снимките се убедливи, привлечни и полесно се создаваат од кога било, а можат да предизвикаат моќни емотивни реакции. Еден резултат од таквата ситуација е што станаа моќни средства за ширење мисинформации и дезинформации.

До денес, расправата за сликите во контекст на мисинформациите и дезинформациите се фокусираше или на техниките на верификација или, од неодамна, првенствено на видеата со „длабоки фалсификати" (deepfake video). Пред да ги разгледаме длабоките фалсификати (тие се тема на следното поглавје), потребно е да дознаеме повеќе за почестите, не толку технички сложени начини на користење на заведувачки фотографии и видеа, особено оние што се прикажани надвор од нивниот изворен контекст.

Со оглед на распространетата употреба на визуелни материјали во обидите да се влијае врз јавниот дискурс или да се манипулира со него, новинарите мора да поседуваат основно знаење за верификација на слики и со способност критички да ги разгледуваат и оценуваат сликите за да разберат како и зошто се употребуваат. Ова поглавје се концентрира на развојот на вториот комплет вештини и се потпира на рамката што ја развивме во Лабораторијата за визуелни социјални медиуми.

Надградба на верификацијата

Во Лабораторијата за визуелни социјални медиуми, фокусирани сме на разбирањето на улогата на онлајн сликите во општеството. Главно сме фокусирани на неподвижните слики, категорија што опфаќа широк дијапазон на различни видови слики: Фотографии, композитни слики и колажи, „мимови“, графички прикази и слики и снимки на екрани (screenshots), се само некои од нив. Справувањето со визуелното мисинформирање и дезинформирање бара свои специфични стратегии. До сега, верификацијата на слики од новинарите се фокусирање дали сликата прикажува тоа што тие мислат дека прикажува. Во првиот „Прирачник за верификација“, Трушар Баро (Trushar Barot) исцрта четири основни принципи за верификација на слики, и тие ја задржуваат својата вредност. Првиот нацрт „Водич за верификација на визуелни материјали“ е друг корисен извор што се потпира на тие принципи преку фокус на пет прашања што се однесуваат на фотографиите и видеата:

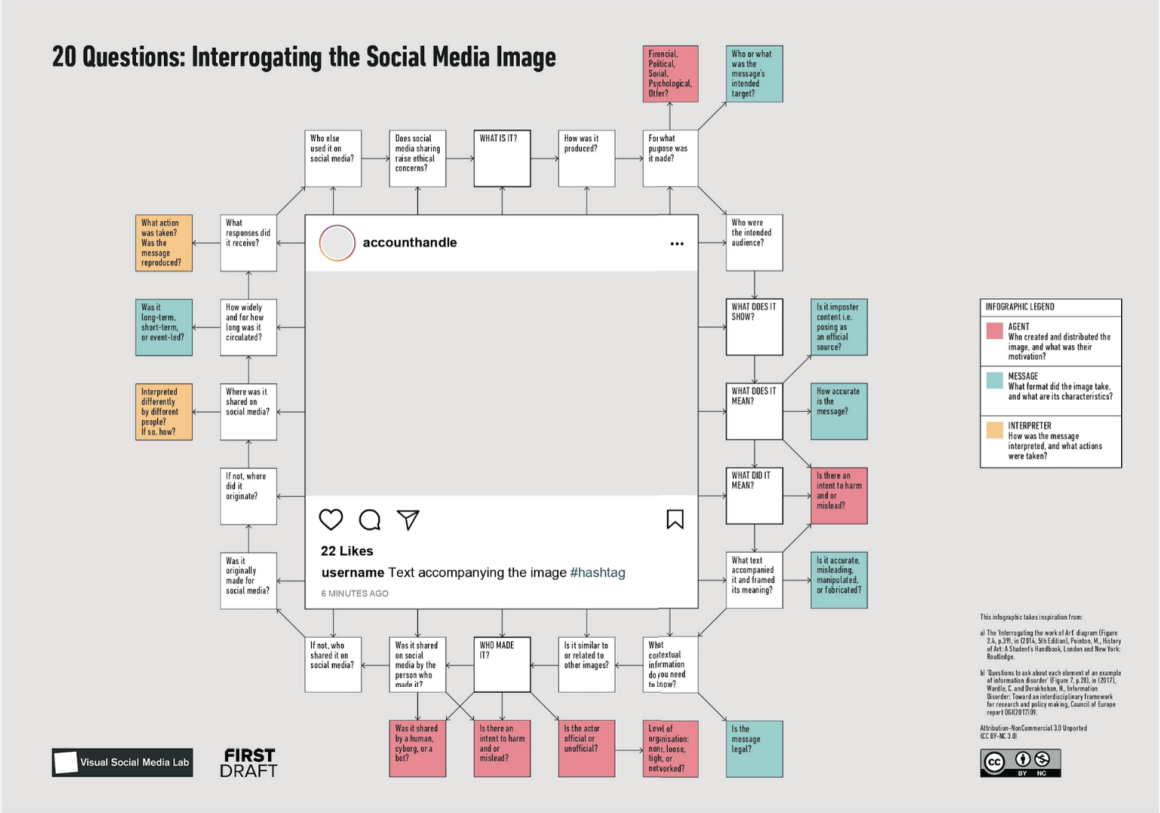
1. Дали тоа што го гледате е изворната верзија?
2. Дали знаете кој ја снимил фотографијата?
3. Дали знаете каде е снимена фотографијата?
4. Дали знаете кога е снимена фотографијата?
5. Дали знаете зошто е снимена фотографијата?

Стандардните алатки што можат да помогнат при истражувањето на фотографии и видеа ги вклучуваат „ИнВИД“ (InVID), пребарувањето на слики на Јандекс (Yandex Image Search), „ТинАј“ (TinEye), пребарувањето на слики на Гугл (Google Image Search) и „Форензикали“ (Forensically). Тие методи за верификација се фокусирани на потеклото на сликата.

Иако тој метод го задржува своето значење, стратегиите и техниките што често се користат за мисинформирање и дезинформирање, како и во еден поширок опсег на форми на медиумски манипулации, значи дека подеднакво значајно е да разгледаме на кој начин се користат и споделуваат сликите и од кого, како и каква е улогата на новинарите во можното натамошно засилување и ширење на проблематичните слики и илустрации.

За да поминеме отаде стандардните форми на верификација на слики, комбинираме методи од историјата на уметноста со прашања наменети специфично за содржини со мисинформации и дезинформации. Нашата рамка, „20 Прашања за испрашување на сликите на социјалните медиуми“ (20 Questions for Interrogating Social media Images), подготвена во соработка со „Фрст драфт“ и новинари, е дополнителна алатка што новинарите можат да ја користат во истражувањето на слики и илустрации.

Распит на сликите на социјалните медиуми



Како што сугерира насловот, рамката содржи 20 прашања што треба да бидат поставени за која било слика или илустрација (фотографија, видео, „гиф“, итн.) на социјалните медиуми, со 14 дополнителни прашања што целат да влезат подлабоко во различните аспекти на мисинформациите и дезинформациите. Прашањата не следат строг редослед, но корисно е следните пет прашања да бидат поставени први:

1. За каква илустрација се работи?
2. Што е прикажано на неа?
3. Кој ја подготвил?
4. Што значело прикажаното во време на изработката?
5. Што значи прикажаното денес?

Прашањата 1 до 3 се слични на воспоставените приоди кон верификацијата и имаат за цел да утврдат за каков тип на слика се работи (фотографија, видео, итн.), што е прикажано на неа и кој ја изработил. Од друга страна, прашањата 4 и 5 не носат во сосема друг правец. Тие внесуваат размислување за значењето што го опфаќа она што е прикажано на сликата, но и сите значења што ги произведува користењето на сликата, вклучително и преку нејзина погрешна идентификација. Ако ги разгледуваме заедно, прашањата 4 и 5 исто така ни овозможуваат да се фокусираме на променливата природа на значењето на сликите и на начините на кои значењата што им ги припишуваме на сликите можат да бидат значајни сами по себе. Тоа не се однесува само на значењето што сликите го добиваат ставени во нов контекст и како тоа придонесува за погрешна идентификација на она што е прикажано на нив, туку и кои се ефектите на таквата погрешна идентификација. Овој приод веќе не се однесува само на верификацијата, туку е повеќе сличен на анализата на значењата на сликите што се вршат во други дисциплини, како што се историјата на уметноста или теоријата на фотографијата.

Во развојот и раната употреба на оваа рамка во новинарството, често слушавме дека новинарите никогаш претходно не размислувале за сликите толку детално. Многумина од нив рекоа дека рамката им помогнала да осознаат дека сликите се комплексна форма на комуникација и дека е потребен јасен метод за нивно преиспитување и преиспитување на нивните значења.

Поголемиот дел од времето, нема да морате да одговорите на сите 20 прашања во рамката за да стекнете целосно разбирање за тоа што се случува со некоја слика. Прашањата се наменети да им се навратите по потреба. Во нашата работа, увидовме дека особено се корисни кога се занимаваме со комплексни, високопрофилни слики и видеа снимени на некој настан од голем интерес, што предизвикал сериозен медиумски интерес и преиспитување. За да покажеме како тоа изгледа во пракса, следат три студии на случаи со високопрофилни примери од Велика Британија и САД.

Студија на случај 1: *Точка на кршење, јуни 2016 година*

За каква илустрација се работи?

Сликата „Точка на кршење“ (Breaking Point) е постер што Партијата на независноста во ВБ (UK Independence Party - UKIP) го користеше во својата кампања во референдумот за излегување од ЕУ во 2016 година. Постерот користеше фотографија снимена од фото-репортерот Џеф Мичел (Jeff Mitchell) во октомври 2015 година, и се однесува на бегалската криза.

Што е прикажано на неа?

Словенечката полиција спроведува долга редица сириски и афганистански бегалци од границата помеѓу Хрватска и Словенија до бегалскиот камп „Брежице“. Постерот користи еден дел од фотографијата со додаден текст „ТОЧКА НА КРШЕЊЕ: ЕУ не разочара сите нас“ и „Мораме да се ослободиме од ЕУ и да ја вратиме контролата на нашите граници“. Бидејќи бегалците на фотографијата се движат, во голем број, кон камерата, визуелниот впечаток е силен.

Кој ја подготвил илустрацијата?

Рекламната агенција „Фемили адвертајзинг Лтд“ (Family Advertising Ltd.) од Единбург, ангажирана од УКИП за нивната кампања за „Брегзит“ (Brexit).

Што значело прикажаното?

УКИП не се обиде погрешно да ја претстави содржината, туку додаде неколку слоеви на дополнителни значења со додавање на слогани. Експлоатирајќи ги постоечките анти-

имиграциски и расистички чувства, манипулацијата беше концентрирана на генерирање додатен страв од имиграцијата и бегалците, врз основа на неосновани тврдења и инсинуации за политиките на ЕУ за заштита на границите.

Што значи прикажаното сега?

Во ноември 2019 година, во предвечерјето на општите избори во Велика Британија, организацијата „Leave.EU“ исто така искористи дел од истата фотографија во една анти-имиграциска илустрација поставена на Твитер, со јасна референца на постерот на УКИП од 2016 година.

Кои други прашања би било полезно да ги поставиме?

Дали актерот е официјален или неофицијален субјект? Дали клучниот актер во создавањето и дистрибуцијата на сликата, УКИП, е официјална политичка партија и не е вид на актер што вообичаено се поврзува со мисинформации и дезинформации.

Дали е слична или е поврзана со други слики? Некои го споредија постерот со нацистичката пропаганда; тој резонира и со претходниот анти-имигрантски имагинариум како и со една долга традиција на политички постери во ВБ на кои се претставени редици, вклучувајќи го и постерот на УКИП, фокусиран на имиграцијата од ЕУ, од 2016 година.

3 заклучоци:

- Официјалните политички партии можат да се јават како актери во ширењето на мисинформации.
- Мисинформациите не вклучуваат нужно лажни слики или дури погрешна идентификација на она што го прикажуваат. Сликите понекогаш можат да се користат како поддршка за порака што погрешно претставува една поширока состојба.
- Некои мисинформации бараат повеќе напори од обична верификација. Постои потреба за критичко преиспитување на начините на кои вистински слики се користат за манипулација, како и што прават и што значат таквите слики.

Примери од медиумското известување за овој случај:

Nigel Farage's anti-migrant poster reported to police – *The Guardian*
Brexit: UKIP's 'unethical' anti-immigration poster — Al-Jazeera
Nigel Farage accused of deploying Nazi-style propaganda as Remain crash poster unveiling with rival vans — The Independent

Студија на случај 2: *Фотографијата од мостот „Вестминстер", март 2017 година*

За каква илустрација се работи?

Еден твит од корисничка сметка на Твитер која наизглед ја води бел Тексашанец, доби значајно медиумско внимание. Подоцна се откри дека со сметката раководи руската „Агенција за истражување на интернет" (Internet Research Agency) и ја користи за ширење погрешни информации и дезинформации. Во твитот беше споделена фотографија снимена непосредно по терористичкиот напад на Вестминстерскиот мост во Лондон (22 март 2017 година).

Што е прикажано на неа?

Жена во муслиманска облека минува покрај група луѓе и едно лице повредено во терористичкиот напад што лежи на улица. Тектот содржи исламофобични конотации, тврдејќи дека жената намерно го игнорира повреденото лице, како и отворено анти-исламски хаштаг.

Кој ја подготвил илустрацијата?

Работник на Агенцијата за истражување на интернет кој раководел со сметката @ SouthLoneStar на Твитер, иако во време на настанувањето на твитот не беше познато дека се работи за сметка на ИРА. Фотографијата е снимена од новинскиот фотограф Џејми Лориман (Jamie Lorriman).

Што значело прикажаното?

Во март 2017 година, изгледаше дека се работи за твит на десничар од Тексас според чија интерпретација на фотографијата е прикажана муслиманка која не се грижи за рането лице. Твитот сугерираше дека тој пример укажува на факт што се однесува пошироко на сите муслимани.

Што значи прикажаното сега?

Денес знаеме дека твитот е доказ дека Агенцијата за истражување на интернет намерно шири исламофобични дезинформации по еден терористички напад.

Кои други прашања би било полезно да ги поставиме?

Какви реакции предизвика*?* Твитот предизвика значајни реакции во мејнстрим медиумите. Десетици весници во ВБ известуваа за него, во некои случаи и во повеќе наврати. Додека најголемиот број од статиите го осудуваа корисникот @SouthLoneStar, известувањето го премести твитот од границите на социјалните медиуми и го претстави на мејнстрим-публиката. Откако сликата се прошири, се јави жената на фотографијата со изјава дека во моментот кога настанала била растроена поради нападите и дека „не само што бев скршена од она што го видов по така шокантен и застрашувачки терористички напад, морав да се справам со шокот да се видам себе на слика поставена на сите социјални медиуми од луѓе што не гледаат подалеку од мојата облека, што извлекуваат заклучоци засновани на омраза и ксенофобија".

Дали е слична или е поврзана со други слики? Сликата што беше најраспространета беше една од седум фотографии на кои беше прикажана истата жена. Другите фотографии јасно покажуваа дека е вознемирена, што беше спомнато само од грст публикации.

Колку широко и колку долго време била во циркулација*?* Дополнителното внимание од мејнстрим медиумите значеше дека твитот имаше голем досег. Сепак, за само неколку дена, неговата циркулација значително забави. Повторно влезе во циркулација во ноември 2017 година, кога беше откриено дека со сметката @SouthLoneStar управува Агенцијата за истражување на интернет. Ноемвриската циркулација беше значително помала во мејнстрим медиумите споредено со март таа година.

3 **заклучоци***:*

- Визуелните дезинформации не секогаш се целосно лажни и можат да вклучуваат елементи што се потпираат на вистината. Фотографијата е вистинска, но нејзиниот контекст е изменет и фалсификуван, и се потпира на тоа што читателот/набљудувачот не може да знае што жената навистина мисли во моментот на снимањето.
- Новинарите треба добро да размислат пред да посветат внимание на такви емоционално напрегнати, контроверзни и потенцијално штетни дезинформации со известување за нив, дури и ако намерите им се добри.
- Треба да се посвети повеќе внимание на исправањето на вестите и статиите што се засновани на дезинформации и да се обезбеди дека првенство ќе има вистинската слика за настаните. Ограниченото известување во ноември значи дека некои читатели можеби не откриле дека твитот всушност е руски обид за дезинформирање.

Примери од медиумското известување за овој случај:

People are making alarming assumptions about this photo of 'woman in headscarf walking by dying man' — *Mirror*
'Who is the real monster?' Internet turns on trolls who criticised 'indifferent' Muslim woman seen walking through terror attack — *Daily Mail*
British MP calls on Twitter to release Russian 'troll factory' tweets — *The Guardian*

Студија на случај 3: *Конфронтацијата пред Меморијалниот центар „Линколн", јануари 2019 година*

За каква илустрација се работи?

Видео на кое се прикажани група ученици од Католичкото средно училиште од Ковингтон (Covington Catholic High School) што учествуваа во „Маршот за живот" против абортусот, и домородниот маж Натан Филипс (Nathan Phillips) кој учествувал во Маршот на домородните народи (Indigenous Peoples March) заедно со други Домородни Американци.

Што е прикажано на неа?

Конфронтација помеѓу еден од учениците од Католичкото средно училиште од Ковингтон и Филипс. Двата протести се сретнаа на плоштадот, при што наводно голема група ученици од Ковингтон со бејзбол-капчиња со натпис „МАГА" (Make America Great Again, MAGA) се соочиле со Филипс. Тоа ја претставува сликата како приказ на сам Домороден Американец што се спротивставува на топла млади силеџии од алтернативната десница (alt-right).

Кој ја подготвил илустрацијата?

Првото објавување на видеото е на Инстаграм, од страна на еден учесник во Маршот на домородните народи. Видеото беше прегледано скоро 200,000 пати. Неколку часа подоцна, видеото беше поставено на Твитер, каде што имаше 2,5 милиони прегледи пред да биде избришано од изворната корисничка сметка. Видеото потоа беше повторно објавено на повеќе различни социјални медиуми, со што го привлече вниманието на мејнстрим медиумите. За помалку од 24 часа беа објавени неколку статии за видеото.

Што значеше прикажаното?

Иницијалниот наратив што се прошири на интернет го претстави видеото како директен судир помеѓу Филипс и учениците, при што на учениците се гледаше како намерно да го предизвикуваат и да му се „опколуваат" Филипс.

Што значи прикажаното сега?

Многу подолго видео од истата средба, што се појави неколку дена по првото видео, прикажа многу покомплексна слика на настанот. Во меморијалниот комплекс во моментот се наоѓала и група од Црни Хебрејски Израелити (Black Hebrew Israelites) кои ги предизвикувале минувачите, вклучувајќи ги и учениците од Ковингтон и учесниците на Маршот на домородните народи. Тоа довело до вжештена ситуација помеѓу сите три групи, а Филипс наводно се обидувал да ја смири ситуацијата. Првото видео почнува токму во тој момент.

Кои други прашања би било полезно да ги поставиме?

Кои информации за контекстот треба да ги знаете*?*

Без подолгото видео и знаењето дека Црните Хебрејски Израелити биле присутни и активно го поттикнувале судирот, се губи секаков контекст. Иако студентите се фатени на снимката како извикуваат расистички изјави, тоа што водело кон такво однесување е многу покомплицирано од едноставната претстава дека алт-десничарски тинејџери нападнале постар домороден маж.

На кои социјални медиуми била споделена*?*

Иако видеото изворно беше споделено на Инстаграм од учесник на Маршот на домородните народи, таму доби ограничено внимание. Потоа беше преобјавено на Твитер и Јутјуб од други корисници, и тоа во огромна мера ја засили свеста за неговото постоење и го обезбеди вниманието на мејнстрим медиумите. Оттаму, вниманието дојде со преобјавувањата, а не од оригиналното видео на Инстаграм.

3 **заклучоци***:*

- Кога такви емоционално набиени визуелни материјали се шират со голема брзина на интернет, лесно е да се изгуби оригиналниот контекст што овозможува површен, реакционерен онлајн наратив да ја преземе контролата.
- Гледано наназад, некои новинари тврдеа дека иницијалните статии долеваа гориво на контроверзите и му дадоа дополнителен импулс на погрешниот наратив. Тоа сугерира дека, без соодветна истрага, мејнстрим медиумите можат ненамерно да продолжат да ја шират дезинформацијата.
- Брзината со која видеото се шириле на интернет значеше дека многу од мејнстрим медиумите „паднаа“ на наратив промовиран на социјалните медиуми, без дополнителна истрага. Многу информативни веб-страници беа принудени да ги повлечат или да ги корегираат своите статии кога се појави винстинската верзија на настаните, а некои од нив беа тужени на суд.

Примери од медиумското известување за овој случај:

Native American Vietnam Vet Mocked And Surrounded By MAGA Hat-Wearing Teens – *UNILAD*
Outcry after Kentucky students in Maga hats mock Native American veteran – *The Guardian*
Fuller video casts new light on Covington Catholic students' encounter with Native American elder – *USA Today*

Заклучок

Визуелните материјали имаат голем удел во она што се споделува на социјалните медиуми. Новинарите мора да поседуваат способност критички да ги разгледуваат и оценуваат сликите за да можат да ги откријат значајните содржини и намери. Брзината со која визуелните мисинформации можат да бидат споделени понатаму ја нагласува потребата новинарите да бидат внимателни и да обезбедат дека целосно ќе ги истражат приказните поврзани со слики пред да објават нешто. „20 Прашања за испрашување на сликите на социјалните медиуми“ е дополнителна алатка за новинарите што истражуваат слики, особено ако приказната првенствено е фокусирана на некаков визуелен елемент. Не секое од прашањата во рамката е релевантно за секоја слика, но петте основни прашања даваат цврста основа и се надградба на основните вештини за верификација, со цел да се развие поточно и подетално известување.

АНЕКС

Подолу е дадена целата листа од 20 прашања во рамката, вклучувајќи и 14 подготвителни прашања фокусирани специфично на мисинформациите и дезинформациите. Како што веќе спомнавме, постојат пет прашања што е корисно да бидат поставени први (задебелени на листата). Подготвителните прашања се однесуваат или на агентот, или на пораката или на толкувачот на мисинформацијата и дезинформацијата:

- АГЕНТ (А) – Кој ја создал и дистрибуирал сликата и кои се неговите/нивните мотиви?
- ПОРАКА (М од message) - Кој е форматот на сликата и какви карактеристики има?
- ТОЛКУВАЧ (I од interpreter) – како е интерпретирана пораката, кои дејства се преземени?

1. За што се работи?
2. Како е произведена?
3. Со каква цел е произведена?
    а. А – Финансиска, политичка, општествена, психолошка или друга?
    б. М–Кој или што е посакуваната цел на пораката?
4. Која е саканата публика?
5. Што прикажува?
6. Што значи?
    а. М – Дали се работи за натрапничка содржина, т.е. позира како официјален извор?
    б. М – Колку е точна пораката?
7. Што значела?
    а. А – Дали постои намера да наштети или да заведе?
8. Со каков текст е проследена илустрацијата за да го врами нејзиното значење?
    а. М – Дали е точна, заведувачка, манипулирана или фабрикувана?
9. Кои информации за контекстот треба да ги знаете?
    а. М – Дали пораката е законита?
10. Дали е слична или е сродна на други илустрации?
11. Кој ја создал?
    а. А – Дали актерот е официјален или неофицијален?
    б. А – Ниво на организација: нема, слаба, цврста, или вмрежена?
12. Дали е споделена на социјалните медиуми од лицето што ја создало?
    а. А – Дали е споделена од човек, киборг или бот?
    б. А – Дали постои намера да наштети ли заведе?
13. Ако не, кој ја споделил на социјалните медиуми?
14. Дали изворно е создадена за социјалните медиуми?
15. Ако не, од каде потекнува?
16. Каде на социјалните медиуми е споделена?
    а. И – Дали различни луѓе различно ја толкуваат? Ако да, како?
17. Колку широко циркулирала и колку долго време?
    а. М – Дали е долгорочна, краткорочна, или врзана за одреден настан?
18. Какви одговори предизвикала?
    а. И – Какви дејства биле преземени? Дали пораката е репродуцирана?
19. Кој друг ја искористил на социјалните медиуми?
20. Дали споделувањето на социјалните медиуми повлекува етички прашања?

Рамката е инспирирана од:

1. Дијаграмот «Interrogating the work of Art" diagram (Figure 2.4, p.39), in (2014, 5th Edition), Pointon, M. History of Art: A Student's Handbook, London and New York: Routledge.
2. "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(2017)09.

6. Како да размислуваме за „длабоките фалсификати“ и новите технологии за манипулација

Автор: Сем Грегори

Сем Грегори *(Sam Gregory) е програмски директор во „Витнес“ (WITNESS, www.witness.org), организација што им помага на луѓето во користењето на видеото и технологијата во борбата за човекови права.*
Наградуван технолог и заговарач, тој е експерт во областа на нови форми на погрешни/дезинформации погонети од вештачката интелигенција (ВИ), и предводи во работата на новите можности и закани за активизмот и новинарството. Тој исто така е ко-претседавач на експертската група на „Партнерство за ВИ“ (Partnership on AI) фокусирана на ВИ и медиумите.

Летото 2018 година, професорот Сивеј Лији (Siwei Lyi) од Универзитетот во Олбени (University of Albany), еден од водечките истражувачи на длабоките видео фалсификати, објави труд што покажува дека лицата претставени во видео со длабински фалсификат не трепкаа со исто стапка како вистинските луѓе. Тоа тврдење наскоро беше пренесено од „Фаст компани“ (Fast Company), „Њу Сајентист“ (New Scientist), „Гизмодо“ (Gizmodo), СиБиЕс Њуз (CBS News) и други, што предизвика многу луѓе да почнат да мислат дека сега имаат потврден начин за препознавање на длабоките фалсификати.

Сепак, само неколку недели по објавувањето на трудот, истражувачот доби видео снимки на кои лице обработено во длабински фалсификат трепка како човек. Денес тој совет не е ниту корисен ниту точен. Во тој момент се работеше за „Ахилова петица“ на алгоритамот за креирање длабоки фалсификати, поради податоците за учење што ги користеше. Неколку месеци подоцна, тоа веќе не беше валидно.

Примерот илустрира една клучна вистина за детектирањето и верификацијата на длабоките фалсификати: Техничките приоди се корисни се додека синтетичките медиуми неизбежно не прилагодат своите техники. Никогаш нема да постои совршен систем за детекција на длабоки фалсификати.

Прашањето е, како новинарите да верификуваат длабоки фалсификати и други форми на синтетички медиуми?

Првиот чекор е да ја разбереме природата на работата, која наликува на играта на мачка и глушец, и да бидеме свесни за развојот на технологијата. Второ, новинарите треба да ги научат и да ги применуваат основните техники и алатки за верификација за да истражат дали некоја содржина била подложена на злонамерна манипулација или е синтетички генерирана. Приодите за верификација на слики и видеа детално се обработени во првиот „Прирачник за верификација“, како и во ресурсите за визуелна верификација на „Фрст драфт“ и се применливи. Тоа значи дека способноста да се верификува автентичноста на некоја фотографија или видео е подеднакво значајна како и способноста да се докаже дека биле предмет на манипулација.

Ова поглавје ги надградува основните пристапи за верификација на видеоизмами. Сепак, најпрво е значајно да имаме основно разбирање за тоа што се видеоизмами и синтетички медиуми.

Што се длабоките фалсификати и синтетички медиуми?

Длабоките фалсификати се нова форма на аудиовизуелна манипулација што овозможува креирање на реалистични симулации на нечие лице, глас или движења. Тие овозможуваат да направите да изгледа како некој да изговорил или направил нешто што не изговорил или не направил. Нивната изработка станува се поедноставна, бара се помалку изворни слики, и сè повеќе се комерцијализираат. Во моментов, длабоките фалсификати доминантно удираат врз жените, и се користат за создавање на сексуални слики и видеа со ликот на одредено лице, без нивна согласност. Постојат стравови дека длабоките фалсификати ќе имаат многу пошироко влијание во целото општество и во процесите на собирање и верификација на вестите.

Длабоките фалсификати се само една нова појава во семејството на техники за генерирање на синтетички медиуми помогнати од вештачката интелигенција (ВИ). Овој сет на алатки и техники го овозможува создавањето на реалистични претстави на луѓе што прават или говорат работи што никогаш не ги направиле или изговориле, реалистични престави на луѓе/објекти што никогаш не постоеле, или настани што никогаш не се случиле.

Технологијата за синтетички медиуми во моментов ги овозможува следните форми на манипулација:

- Додавање и отстранување на предмети во видео снимка.
- Менување на позадината во видеото. На пример, да се променат временските услови за видеото што е снимено во лето да изгледа како да е снимено во зима.
- Симулирање и контрола на реалистична видео презентација на усните, фацијалните експресии или движењата на телото на едно одредено лице. Иако расправата за длабоките фалсификати општо се фокусира на лицата, слични техники се применуваат и на телесните движења или на одделни делови од лицето.
- Генерирање на реалистична симулација на нечиј глас.
- Модификација на постоечки глас со „гласовна прекривка“ од друг род, или од друго лице.
- Создавање на реалистична но целосно фабрикувана фотографија од непостоечко лице. Истата техника може да се примени, иако тоа е далеку помалку проблематично, за креирање на лажни хамбургери, мачки, итн.
- Пренесување на реалистично лице од една индивидуа на друга, таканаречен „длабински фалсификат“ (deepfake).

Наведените техники првенствено, но не исклучиво, зависат од една форма на вештачка интелигенција позната како „длабоко учење“ (deep learning) и од таканаречените „ГАН“ мрежи (од Generative Adversarial Network - GAN).

За генерирање на синтетичка медиумска содржина, почнувате со собирање на слики или видео од лицето или предметот што сакате да го фалсификувате како извор. ГАН го развива фалсификатот - сè едно дали се работи за видео симулација на вистинска личност или замена на физиономии - со користење на две мрежи. Едната мрежа генерира веродостојни рекреации на изворните слики, додека втората работи на детекција на фалсификатите. Наодите на втората мрежа се враќаат во мрежата што работи на создавање на фалсификатите, помагајќи и да ја подобри својата работа.

Во моментот на пишување на овој текст, многу од тие техники - особено создавањето на длабоки фалсификати - сè уште бараат значителна компјутерска моќ, знаење за начините на прилагодување на моделот, а често и користење на компјутерска графика и обработка (Computer Graphics and Imaging - CGI) во постпродукција за подобрување на конечниот резултат.

Сепак, и покрај постоечките ограничувања, луѓето лесно се измамени од симулирани медиуми. На пример, истражувањето на проектот „ФејсФорензикс++“ (FaceForensics++) покажува дека луѓето не можат конзистентно да ги откријат денешните форми на модификација на движењата на усните што се користат за да се синхронизираат движењата на устата со нова аудио снимка. Тоа значи дека луѓете немаа вродена способност за откривање на манипулации со синтетички медиуми.

Треба да се забележи и дека аудио синтезата напредува многу побрзо од очекуваното и станува достапна како комерцијална услуга. На пример, апликациско програмскиот интерфејс (АПИ) за претворање на текст во говор на Гугл Клауд (Google Cloud Text-to-Speech API) ви овозможува да претворите некој текст во аудио запис со човечки глас што звучи реалистично. Неодамнешните истражувања се фокусираа и на можноста за претворање на текст во комбиниран видео/аудио запис во видео интервју.

На крај, сите технолошки трендови и трендовите за комерцијализација посочуваат дека производството на убедливи синтетички медиуми ќе биде сè полесно и поефтино. На пример, следната слика покажува со која брзина напредува технологијата за генерирање на човечко лице.

Credit: EFF

Поради тоа што природата на овие мрежи наликува на брканица на мачка и глушец, тие постојано се подобруваат со текот на времето бидејќи се хранат со податоците и од успешните фалсификати и од успешната детекција. Тоа бара голема претпазливост во врска со успешноста на методите за детекција.

Постоечкиот пејсаж на длабоки фалсификати и синтетички медиуми

За сега, длабоките фалсификати и синтетичките записи не се многу раширени надвор од имагинариумот на неконсензуалниот секс. Извештајот на Лабораторијата „ДипТрејс“ (Deep Trace Lab) за нивното присуство посочува дека, според состојбата од септември 2019 година, преку 95% од длабоките фалсификати се од тој тип и вклучуваат познати и славни личности, порно актерки или обични луѓе. Дополнително, луѓето почнуваат да ги оспоруваат и вистинските содржини прогласувајќи ги и отфрлајќи ги како длабоки фалсификати.

На работилниците на ВИТНЕС ги разгледувавме потенцијалните вектори на закани со претставници на граѓанското општество од различни области, вклучувајќи и локални медиуми, професионални новинари и проверувачи на факти, како и истражувачи на мисинформациите и дезинформациите и специјалисти по разузнавање на отворени извори (Open-Source Intelligence OSINT). Тие ги приоритизираа областите во кои новите форми на манипулации можат да ги прошират постоечките закани, да воведат нови закани, да ги изменат постоечките закани или да зајакнат други закани. Тие идентификуваа закани за новинарите, проверувачите на факти и истражувачите на отворени извори, како и потенцијални напади врз нивните работни процеси и процедури. Ги потцртаа и предизвиците што ги носи изјавата „тоа е длабински фалсификат“ како реторички блиска на изјавата „тоа е лажна вест“.

Во сите контексти, го посочија значењето на прегледувањето на длабоките фалсификати во контекст на постоечките приоди кон проверката на факти и верификацијата. Длабоките фалсификати и синтетичкитемедиуми ќе се интегрираат во постоечките конспиративни и кампањи за дезинформирање, извлекувајќи поуки од менливите тактики (и одговори на нив) во таа област, сметаат претставниците на граѓанското општество.

Следат неколку од посочените специфични закани :

- Ќе биде нападната репутацијата и кредибилитетот на новинарите и граѓанските активисти, надградувајќи се на постоечките форми на вознемирување и насилство на интернет чија доминантна цел се жените и малцинствата. Веќе се забележани напади врз жени новинарки со користење на модификувани видеа, како што беше случај со нападот на познатата индиска новинарка Рана Ајуб (Rana Ayyub).
- Јавни личности ќе се соочат со слики со сексуална содржина за кои не дале согласност и родово-засновано насилство, како и со други начини на користење на тн. „веродостојни двојници“ (credible doppelgangers). Локалните политичари можат да бидат особено ранливи, затоа што ги има на многу фотографии а на располагање имаат помала институционална структура за поддршка од политичарите на национално ниво што би им помогнала во одбраната од напади со синтетички медиуми. Исто така, тие често се клучни извори во известувањето за теми што произлегуваат од локално и се шират на национално ниво.
- Присвојување на познати брендови со фалсификувани монтирани делови од видеа и други начини на кои информативни медиумски, владини, корпоративни или невладини брендови можат лажно да се припојат кон некоја содржина.
- Обиди за вметнување на манипулирани, кориснички содржини во циклусите на вести, комбинирани со други техники како што се хакирање на изворите (source-hacking) или споделување на манипулирани содржини со новинари во клучни моменти. Вообичаено, целта е новинарите да помогнат во ширењето на таквите содржини.
- Користење на слабостите на процесите на собирање на вестите и известувањето, како што се директните преноси од далечина со една камера (како што посочи тимот на Ројтерс УГЦ (Reuters UGC team) и собирањето на материјали во контексти што се тешки за верификација, на пример, од зони на воени дејства и други места.h

- Како што се шири нивната употреба а нивната изработка станува полесна, видеоизмамите ќе придонесат кон поплава на лажни информации што ќе ги преплави организациите што се занимаваат со верификација и проверка на факти со содржини што треба да ги верификуваат или раскринкаат. Таквото оптоварување може да им го одземе вниманието.
- Организациите што известуваат или верификуваат информации ќе се најдат под притиок да докажат дека нешто е вистина, како и да докажат дека нешто не е фалсификувано. Оние што ја имаат моќта ќе можат да се користат со принципот на веродостојно негирање за каква било содржина со изјави дека се работи за длабински фалсификат.

Почетна точка во верификацијата на длабоките фалсификати

Знаејќи ја природата на медиумската форензика и на надоаѓачките технологии на длабоки фалсификати, мораме да прифатиме дека отсуството на докази дека нешто било манипулирано нема да се смета за конечен доказ дека медиумот не бил менуван и манипулиран.

Новинарите и истражувачите треба да усвојат менталитет на одмерен скептицизам кон фотографиите, видео и аудио снимките. Мораат да претпостават дека тие медиумски форми ќе бидат под почест предизвик како што се зголемува знаењето за и стравото од видеоизмамите. Основно е развивањето на добро познавање на алатките за медиумска форензика.

Знаејќи го сето тоа, приодот кон анализата и верификацијата на видеоизмамите и манипулациите со синтетички медиуми треба да вклучува:

1. Преглед на содржините за да се откријат вообичаените дефекти или дисторзии кај синтетичките медиуми.
2. Примена на постоечките приоди за верификација и форензика на видео материјали.
3. Користење на новите приоди засновани на ВИ и новите форензички приоди, секогаш кога е можно.

Преглед за вообичаени дефекти или дисторзии

Ова е најмалку робусен приод кон идентификацијата на длабоки фалсификати и други модификации на синтетички медиуми, особено знаејќи ја еволутивната природа на технологијата. Сепак, лошо изработените длабоки фалсификати или синтетички содржини можат да содржат докази за видливи грешки. Во потрагата по длабоки фалсификати треба да внимавате на следното:

- Можни дисторзии на челото/линијата на косата кога лицето се движи надвор од фиксираното поле на движење. Недостиг на детали на забите.
- Премногу мазна кожа. Отсуство на трепкање.
- Статичен говорник без какво било вистинско движење со главата или гестикулација. Дефекти видливи кога лицето се врти од анфас во профил.

За некои од тие дефекти во моментов постои поголема веројатност да бидат забележани со анализа кадар-по-кадар, што значи дека може да помогне извлекувањето на серија на кадри што ќе бидат прегледани индивидуално. Тоа нема да биде случај со дефектите при движење од анфас во профил - тие најдобро се забележуваат во секвенца, што значи дека треба да ги примените двата приоди.

Примена на постоечките приоди за верификација

Како и кај другите форми на медиумски манипулации и „плитки фалсификати“ (shallowfake), како што се монтирани видеа или видеа поставени во погрешен контекст, треба да го втемелите пристапот во потврдените практики за верификација. Постоечките практики за верификација од отворени извори на информации (ОСИНТ) остануваат релевантни, а добра стартна позиција нудат поглавјата и студиите на случај од првиот Прирачник посветени на верификација на слики и видео. Бидејќи повеќето длабоки фалсификати и модификации во моментов не се целосно синтетизирани туку се потпираат на менување на изворно видео, можете да искористите индивидуални кадри од некое видео и да побарате други верзии со реверзибилно пребарување на слики. Видеото можете да го проверите и така што ќе споредите дали на него се прикажани истиот пејсаж и знаменитости како на „Гугл Стрит вју“ (Google Street View).

Слично, приодите засновани на разбирање на начините на кои се споделува содржината, од кого и како, можат да откријат информации што ќе помогнат да решите дали да и верувате на сликата или видеото. Основите на утврдувањето на изворот, датумот и времето на создавање и мотивите зад некоја содржина се клучни во утврдувањето дали таа документира вистински настан или личност. (За темелите на овој приод, видете во водичот на „Фрст драфт“). Како и секогаш, нужно е да го контактирате лицето или лицата што се појавуваат во видеото за да побарате коментар и да проверите дали можеби имаат конкретни информации што можат да ја потврдат или негираат неговата автентичност.

Владите, академската заедница, платформите и новинарските иновациски лаборатории постојано развиваат нови алатки како помош во детектирањето на синтетички медиуми и да го прошират арсеналот на алатки за медиумска форензика. Во повеќето случаи, на тие алатки треба да се гледа како на сигнали што ќе го дополнат приодот кон верификацијата заснована на добри практики.

Алатките како што се „ИнВИД“ и „Форензикали“ помагаат и при верификацијата фокусирана на потеклото и при ограничената форензичка анализа.

Бесплатните алатки во оваа област ги вклучуваат:

- FotoForensics: Алатка за форензика на слики што вклучува можност за Анализа на ниво на грешка (Error Level Analysis) за да се види каде во видеото можеби се додадени нови елементи.
- Forensically: Комплет алатки за детектирање на клонирање, анализа на ниво на грешка, мета-податоците на сликата и повеќе други функции.
- InVID: Додаток за прелистувачи што овозможува фрагментирање на видеата во единечни кадри, реверзибилно пребарување на слики на повеќе пребарувачи одеднаш, лупа за зголемување и преглед на кадрите и сликите, и примена на форензички филтри на неподвижни слики.
- Reveal Image Veri cation Assistant: Алатка што располага со широк опсег на алгоритми за детекција на менување на слики, плус анализа на мета-податоци, гео-лоцирање со ГПС (GPS), EXIF извлекување и интеграција на мали слики со реверзибилно пребарување на слики на Гугл.
- Ghiro: Онлајн дигитална форензичка алатка со отворен изворен код.

Забележете дека скоро сите овие алатки се наменети за верификација на слики, а не на видео. Тоа е слабост во делот на форензиката, што значи дека за верификација на видео сè уште е потребно да се извадат единечни кадри за анализа, нешто во што може да ви помогне „ИнВИД“. Овие алатки ќе бидат најуспешни во работата со некомпресирани видеа со висока резолуција од кои, на пример, се отстранети или додадени некои предмети. Што повеќе видеото е компресирано, повторно зачувувано или споделувано помеѓу социјалните медиуми и платформите за споделување видео, нивната корисност ќе опаѓа.

Ако барате нови форензички алатки за да се справите со постоечките предизвици во областа на визуелната форензика, а евентуално и со длабоките фалсификати, една опција ви се алатките што ги споделува академската заедница. Еден од водечките истражувачки центри на Универзитетот во Неапол обезбедува онлајн пристап до нивниот програмски код за детектирање, меѓу другото, и на трагите што ги оставаат користените камери (Noiseprint), детектирање на „накалемено" видео (Splicebuster) и детектирање на копирање во и отстранување на снимки надвор од видеото.

Со развојот на синтетичките медиуми, ќе се рафинираат нови форми на рачна и автоматска форензика и ќе бидат интегрирани во постоечките алатки за верификација со кои служат новинарите и проверувачите на факти, а потенцијално и во приодите фокусирани на платформите. Значајно е новинарите да се трудат да го ажурираат своето познавање на достапните алатки, но истовремено и да не станат премногу зависни од нив.

Нови приоди кон медиумската форензика засновани на ВИ

До почетокот на 2020 година, не постоеја тестирани, комерцијални алатки за детекција засновани на ГАН. Сепак, треба да очекуваме дека некои такви алатки ќе влезат на пазарот или како додатоци (plug-in) или како алатки на платформите во 2020 година. За актуелен преглед на состојбата во областа на медиумска форензика, вклучувајќи ги и таквите алатки, треба да го прочитате извештајот на Луиза Вердолива (Luisa Verdoliva) „Media Forensics and Deepfakes: An overview".

Тие алатки главно ќе се потпираат на постоењето на податоци за учење (примери) на синтетички медиуми засновани на ГАН, што потоа ќе го користат за детектираат други примери произведени со користење на иста или слична техника. На пример, форензичките програми како што е „ФејсФорензикс++" (FaceForensics++) генерираат фалсификати со користење на комерцијални алатки за длабоки фалсификати а потоа ги користат големите количества на лажни слики како податоци за тренинг на алгоритмите за детекција на фалсификати. Тоа значи дена можеби нема да бидат толку успешни во детектирањето на најновите методи и техники за фалсификување.

Алатките ќе бидат многу попогодни за детекција на медиуми генерирани со ГАН од постоечките форензички техники. Тие, исто така, ќе ги заменат новите форми на алатки за медиумска форензика што подобро се справуваат со напредокот во синтезата. Сепак, нема да бидат сто отсто сигурни, со оглед на адверсаријалната природа на развојот на синтетичките медиуми. Еден заклучок е дека секаква индикација за постоење на синтеза треба да се провери два пати и да се потврди со други пристапи за верификација.

Длабоките фалсификати и синтетичките медиуми еволуираат со голема брзина а технологиите стануваат сè пошироко достапни, комерцијализирани и лесни за употреба. Потребно им е многу помалку изворна содржина за да создадат фалсификат од што би можеле да очекувате. Иако се појавуваат нови технологија за детекција и се интегрираат во платформите и во алатките за новинарите и истражувачите на ОСИНТ, најдобар начин да се пристапи кон верификацијата е користењето на постоечките пристапи кон слики/видео, и нивно дополнување со форензички алатки што можат да детектираат манипулации со сликите. Вербата во способноста на човечкото око не е најсигурна стратегија!

7. Следење и известување во затворени групи и апликации за испраќање и примање пораки

Автор: Клер Вордл

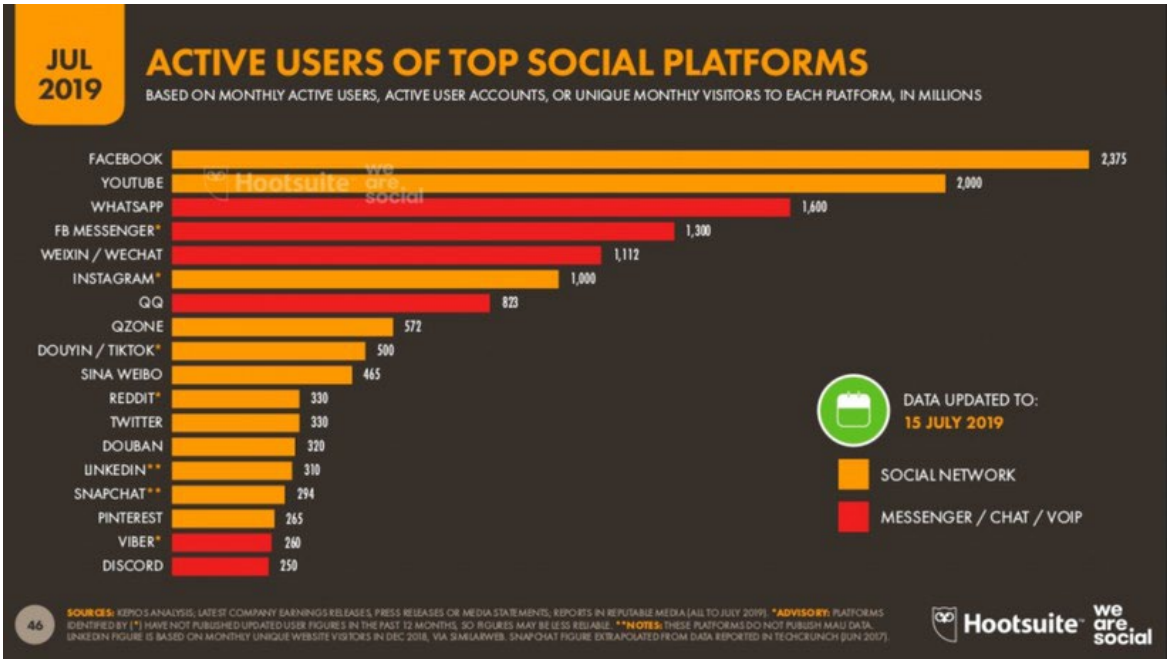
Клер Вордл *(Claire Wardle) раководи со одделот за стратегиски правци и истражување во „Прв нацрт" (First Draft), глобална непрофитна организација што им дава поддршка на новинарите, членовите на академската заедница и технолозите во наоѓањето одговори на предизвиците поврзани со довербата и вистината во дигиталната ера. Работела како соработник на Шоренстеин центарот за медиуми, политика и јавни политики на Кенеди школата на Харвард (Fellow at the Shorenstein Center for Media, Politics and Public Policy, Harvard's Kennedy School), Директор за истражувања на Тоу центарот за дигитално новинарство на Школата за пост-дипломски студии по новинарство на Универзитетот Колумбија (Tow Center for Digital Jounalism, Columbia University's Graduate School of Journalism), и раководител за социјални медиуми во УНХР, Агенцијата за бегалци на ОН.*

Во март 2019 година, Марк Закерберг (Mark Zuckerberg) говореше дека Фејсбук ќе „се врти кон приватноста", што значеше дека компанијата ќе стави акцент на Фејсбук групите, како признание дека луѓето сè повеќе комуницираат со помал број луѓе во затворени кругови. Во последниве неколку години, на луѓето што работат во таа област им стана јасно значењето на помалите групи за социјална комуникација.

Во ова поглавје, ќе ги опишам различните платформи и апликации, ќе говорам за предизвиците што ги носи следењето на таквите простори, и ќе завршам со дискусија за етиката на занимавањето со таа работа.

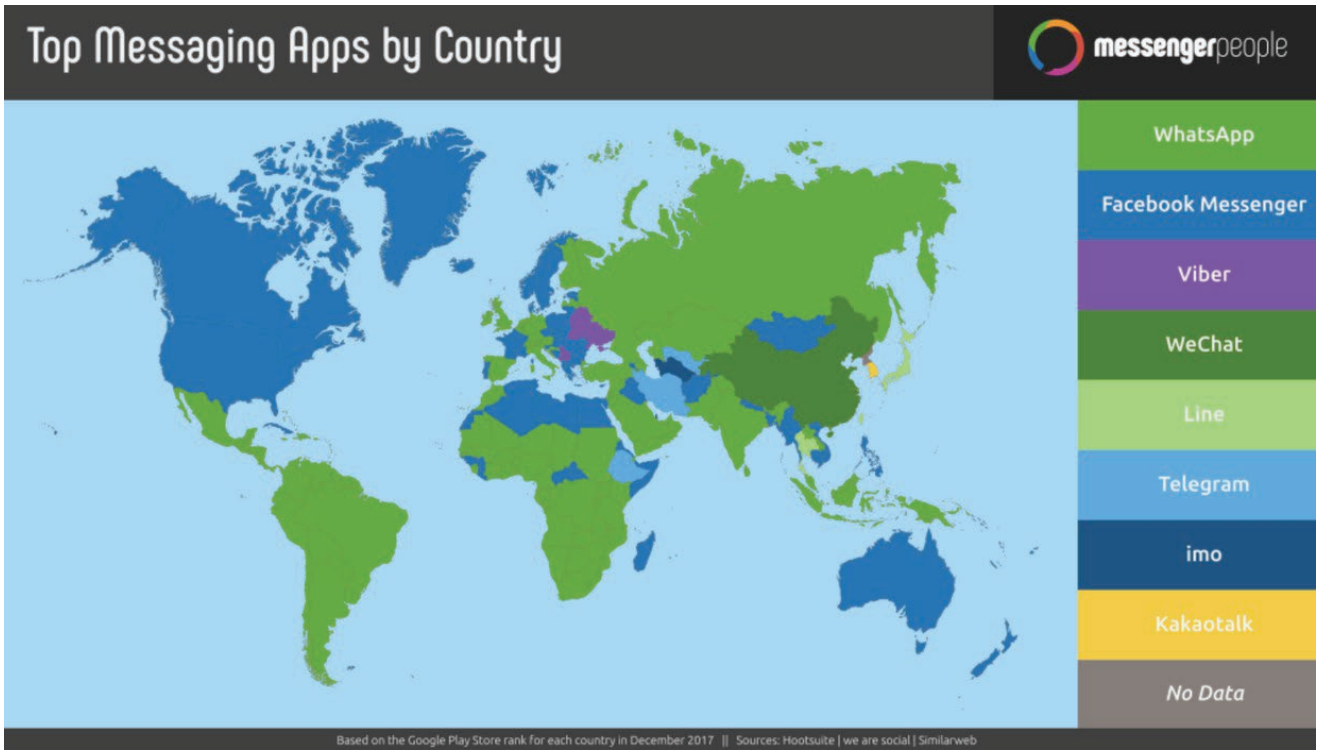
Различни платформи и апликации

Неодамнешно истражување на организацијата „Ние сме општествени" („We Are Social") покажува постојана доминација на Фејсбук и на Јутјуб, но следните три најпопуларни платформи се „ВотсАп" (WhatsApp), „ФБ Месинџер" (FB Messenger) и „ВиЧет" (WeChat).На следната слика е прикажана листа на социјалните платформи според бројот на активни корисници



Во многу делови на светот, апликациите за размена на пораки станаа доминантен извор на вести за голем број потрошувачи, и тоа особено се однесува на „ВотсАп“, на пример, во Бразил, Индија и Шпанија.

Секако, ВотсАп и ФБ Месинџер се глобално популарни, но во некои земји доминираат алтернативни решенија. На пример, во Иран тоа е „Телеграм“ (Telegram). Во Јапонија е „Лајн“ (Line), во Јужна Кореја е „КакаоТок“ (KakaoTalk) а во Кина е „ВиЧет“.



Најпопуларните апликации за размена на пораки по држава

Сите тие сајтови имаат донекаде различни функционалности, од гледна точка на шифрирањето, карактеристиките на групите или емитувањето, како и дополнителни опции како што се можностите за тргување во апликациите.

Затворени групи на Фејсбук

Постојат три видови групи на Фејсбук (Facebook Groups): Отворени, затворени и скриени.

- Отворените групи можат да се пронајдат со пребарување и секој може да стане член.
- Затворените групи можат да се пронајдат со пребарување, но мора да се пријавите и да бидете примени во членство.
- Скриените групи не можат да се пронајдат со пребарување а се зачленува само со покана.

Сè почесто, луѓето се собираат на Фејсбук во групи, делумно затоа што ги промовира алгоритамот на Фејсбук, но, исто така, затоа што луѓето бираат да го минат времето со познати, или со луѓе што ги делат нивните погледи или интереси.

Дискорд

Според „Статиста“, во јули 2019 година „Дискорд“ (Discord) имал 250 милиони активни корисници месечно (за споредба, „Снеп“ (Snap) имал 294 милиони, „Вајбер“ (Viber) имал 260 милиони, а „Телеграм“ 200 милиони). Дискорд е популарен во заедницата на гејмери, но подледниве години стана познат ако сајт каде луѓето се собираат на „сервери“ (една форма на група во Дискорд) за координирање на кампањи за дезинформирање.

Еден аспект на Дискорд, но и на некои затворени групи на Фејсбук, е дека ќе ви постават прашања пред да бидете примени во групата. Прашањата можат да бидат за вашата професија, вероисповест, политички убедувања или ставови за одредени социјални прашања.

Енкрипција, **групи и канали**

Една причина за популарноста на овие платформи и апликации е што нудат различни нивоа на енкрипција. „ВотсАп“ и „Вајбер“ се најбезбедни во моментов, и нудат енкрипција од почеток до крај на користењето на услугата. Други, како што се „Телеграм“, „ФБ Месинџер“ и „Лајн“, нудат енкрипција но треба самите да ја вклучите.

Некои аппликации имаат групи или канали каде информациите се споделуваат со многу луѓе. Најголемата група на „ВотсАп“ може да има 256 членови. Групите на „ФБ Месинџер“ имаат капацитет од 250 членови. На „Телеграм“, групите можат да бидат приватни или да се пребаруваат јавно, со капацитет од 200 членови. Кога групата ќе го достигне тој број, може да се претвори во супергрупа на која можат да и се приклучат до 75,000 членови. „Телеграм“ нуди и канали, можност за емитување во рамките на апликацијата. Можете да се претплатите на некој канал и да гледате што е постирано на него, но не можете да одговорите со поставување на свои содржини.

Тековно следење

Нема сомнеж дека мисинформациите циркулираат на затворените апликации за испраќање пораки. Тешко е да се даде независна проценка дали на овие платформи има повеќе мисинформации или на социјалните медиуми, затоа што не постои начин да се провери што сè се споделува. Сепак, знаеме дека е проблем, како што покажаа високопрофилни случаи од Индија, Франција и Индонезија. И во САД, за време на престрелките во Ел Пасо и во Дејтон во август 2019 година, имаше примери за гласини и лажни информации што циркулираа на „Телеграм“ и на „ФБ Месинџер“.

Прашањето е дали новинарите, истражувачите, проверувачите на факти, здравствените и хуманитарните работници треба да влезат во таквите затворени групи за да следат дали се јавуваат мисинформации. Ако треба да се таму, како да ја вршат својата задача на етички и на безбеден начин?

Иако вршењето на таа работа поставува значајни предизвици, сепак е можно. Од друга страна, имајте на ум дека многу од луѓето што ги користат таквите апликации го прават тоа токму за да избегнат нивните активности да бидат следени. Ги користат поради енкрипцијата. Очекуваат одредено ниво на приватност. Тоа треба да биде централна позиција за сите што работат во таквите простори. Дури и ако можете да се приклучите и да ги следите, од врвно значење е да бидете свесни за одговорноста што ја имате кон другите учесници во таквите групи кои често не разбираат и не се запознаени што е можно а што не е.

Техники за пребарување

Барањето на таквите групи може да се покаже тешко, затоа што за секоја од нив постојат различни протоколи. За групите на Фејсбук, можете да пребарувате по теми со пребарувачот на Фејсбук и потоа да филтрирате по групи. Ако сакате да користите понапредни „Булови“ оператори за пребарување (Boolean), пребарувајте на Гугл со саканите клучни зборови и додадете site:facebook.com/groups.

На „Телеграм“ можете да пребарувате внатре во апликацијата ако имате „Андроид“ телефон, но не и на „Ајфон“. Постојат компјутерски апликации како што е https://www.telegram-group.com/. Слично е и за „Дискорд“, со сајтови како што е https://disboard.org/search

Одлучување за приклучување и учество

Како што веќе спомнавме, некои од тие групи ќе постават прашања на кои треба да одговорите за да обезбедите влез во нив. Пред да се обидете, треба да зборувате со вашиот уредник или раководител како да одговорите на прашањата. Дали ќе ја кажете вистината за тоа кој сте и зошто сте во групата? Постои ли начин да се пристапи во групата со намерно неодредени одговори? Ако не постои, како ќе ја оправдате одлуката да го сокриете вашиот идентитет (ова може да биде нужно ако сакате да пристапите во група во која тоа што ќе се претставите како новинар може да ја загрози вашата безбедност). Ако влезете во групата, дали ќе придонесувате на каков било начин или само ќе „висите“ таму да пронајдете информации што ќе ги потврдите на друго место?

Одлуки за автоматско собирање содржини од групи

Можно е да се пронајдат „отворени“ групи со пребарување на линкови поставени на други сајтови. Таквите линкови се јавуваат во пребарувачите. Тогаш можат да се употребат компутациски методи за автоматско собирање на содржини од таквите групи. Истражувачи што ги следеа изборите во Бразил и во Индија го направија тоа, а знам, од кажување, и за други организации што се занимаваат со слични активности.

Таа техника им овозможува на организациите истовремено следење на повеќе групи, што често е невозможно на друг начин. Клучно е што така можат да се пронајдат само мал дел од групите, и главно се работи за групи што очајнички бараат пошироко членство што значи дека не се репрезентативни за сите групи. За мене лично тоа повлекува одредени етички прашања. Сепак, постојат рамки што можат да се употребат за да се заштитат податоците, да не се споделуваат со други, и да се отстрани идентитетот на авторите на пораките. Потребни ни се протоколи на ниво на индустрија за вршењето на тој вид на работа.

Линии за барање информации

Една техника е да се воспостави линија со која ќе ја охрабрите јавноста да ви испраќа содржини. Клучно за таква линија е едноставен, јасен повик на дејствување, како и да објасните како планирате да ги користите содржините. Дали е наменета само за следење на трендовите или ќе одговарате со раскринкување откако ќе го истражите тоа што ви го испратиле?

Да се навратиме на етичките прашања кои влијаат го голема мера на работата со затворени апликации за размена на пораки, значајно е да не се занимавата само со „земање“ содржини, или со други зборови, да бидете екстрактивни. И ако ја оставиме етиката настрана на момент, сите истражувања покажуваат дека ако публиките не знаат како се користат нивните „дојави“, веројатноста дека ќе продолжат да ги испраќаат значајно се намалува. Луѓето се поподготвени да помогнат само ако чувствуваат дека ги третирате како партнери.

Друг аспект е колку лесно е да се изиграат линиите за дојави со испраќање на измамнички содржини, или така што едно лице или помала група ќе испраќаат многу примероци од истата содржина за да изгледа дека се работи за многу поголем проблем од што навистина е.

Етиката на известувањето од затворени групи за размена на пораки

Откако ќе ја пронајдете содржината, прашањето е како да известувате за неа. Дали треба да бидете транспарентни за начинот на кој сте ја пронашле? Како дел од нивните упатства за членство во заедницата, многу групи бараат тоа што се разговара во групата да не се споделува со други луѓе. Ако групата е полна со дезинформации, каков ќе биде ефектот од

вашето известување за тоа? Можете ли да ги потврдите наодите во други групи или во онлајн просторот? Ако известите, дали тоа ќе значи да ја доведете вашата безбедност, или безбедноста на колегите и семејството во ризик? Запомнете дека „доксирањето“ (doxxing, објавување на приватни информации за идентификација на некое лице со зла намера) на новинарите и истражувачите (или дури полоши работи) се дел од правилата на дејствување за некои од „поцрните“ групи на интернет.

Заклучоци

Известувањето за и од затворени апликации и групи за размена на пораки е полно со предизвици, па сепак, тие извори ќе добиваат сè повеќе значење како простори во кои се разменуваат информации. Како прв чекор, размислете за прашањата наведени во ова поглавје, разговарајте со колегите и уредниците, и ако вашата редакција нема упатства за вршење на овој вид на известување почнете да работите на такви упатства. Не постојат стандардни правила како да се пристапи кон известувањето. Зависи од приказната, платформата, новинарот и уредувачките правила и упатства на редакцијата. Сепак, значајно е да се разгледаат сите тие детали пред да почнете да се занимавате то тој вид на известување.

7а. Студија на случај: Болсонару во болницата

Автор: Сержиу Литке

Сержиу Литке *(Sérgio Lüdtke) е новинар и уредник во „Прожету Компрова" (Projeto Comprova), коалиција од 24 медиумски организации што соработуваат на истражување на гласините поврзани со јавните политики во Бразил.*
Во 2018 година, „Компрова" разгледуваше сомнителни содржини за претседателските избори во Бразил споделувани на социјалните медиуми и апликациите за размена на пораки.

На 6 септември 2018 година, еден месец пред претседателските избори во Бразил, кандидатот на крајната десница Жаир Болсонару (Jair Bolsonaro) одржа настан во склоп на кампањата во центарот на Жуиз де Фора (Juiz de For a), град со 560,000 жители оддалечен 200 километри од Рио де Жанеиро.

Беше помината една недела откако Болсонару стана предводник на предизборните анкети за првиот круг на претседателските избори. Тој излезе на првото место откако Врховниот изборен суд ја забрани кандидатурата на поранешниот претседател Луиз Инасио Лула да Силва (Luiy Inácio Lula da Silva), претходниот убедлив лидер во анкетите.

Сепак, симулациите покажуваа дека Болсонару губи во вториот круг од три од четирите најдобро рангирани кандидати во анкетите.

Ситуацијата беше загрижувачка за Болсонару, затоа што имаше само два дневни блокови во траење од 9 секунди од бесплатното изборно емитување на ТВ. Изборните правила во Бразил им наложуваат на радио и ТВ станиците да им ослободат бесплатно време на политичките партии да ги претстават своите програми. Времето се распределува во согласност со бројот на пратенички места што секоја од партиите ги освоила на последните избори за Претставничкиот дом. Тоа што Болсонару немаше пратеници значеше дека му следува многу малку бесплатно време. Затоа мораше да се потпре на своите поддржувачи на социјалните мрежи и да води кампања на директни контакти со гласачите на улица.

Во Жуиз де Фора, како и во другите градови што претходно ги беше посетил, Болсонару учествуваше во марш на кој неговите поддржувачи го носеа на раменици. Беше следен од толпа следбеници кога маршот изненадно беше прекинат. Среде толпата, еден маж го нападна и го прободе кандидатот со нож. Сечилото остави длабока рана во стомакот на Болсонару - и ја отвори „Пандорината кутија" на социјалните мрежи.

Се шират гласини и теории на заговор. Некои од нив го обвинуваа Аделиу Биспу де Оливеира (Adélio Bispo de Oliveira), човекот што го прободе Болсонару, за поврзаност со партијата на поранешната претседателка Дилма Русеф (Dilma Rousseff) која беше отстранета од позицијата во 2016 година. Лажни фотографии го прикажуваа напаѓачот сликан со Лула. Тоа што Биспу бил поврзан со левичарката Партија на социјализмот и слободата (Partido Socialismo e Liberdade - PSOL), како и одбивањето на неговите адвокати да кажат кој ги плаќа нивните хонорари, само дополнително ги хранеше тврдењата за постоење на заговор.

Истовремено, видеа и пораки што се обидуваа да го подријат Болсонару добија поголемо внимание на социјалните медиумски платформи. Дел од таквите злонамерни содржини тврдеа дека нападот бил режиран, дека Болсонару бил во болница на лекување од рак, и дека објавените фотографии од операцијата се фалсификати.

Нападот му даде на Болсонару изговор да се повлече од кампањата, но му донесе и подобра позиција во анкетите. (Сè разбира, Болсонару на крај ги доби изборите.)

На 19 септември, нецели две недели по нападот, „Елеисоес сем фејк“ (Eleições sem Fake - избори без лаги), програма за следење на „ВотсАп“ групи создадена од Универзитетот на Минас Жераис, идентификуваше аудио снимка што кружеше на интернет. Аудиото беше споделено од 16 од безмалку 300 групи следени од проектот; некои од нив беа поддржувачи на Болсонару.

Истиот ден нашата организација, „Компрова“, почна да прима, исто така преку „ВотсАп“, барања од читателите да го верификуваме итегритетот на снимката.

На снимката, малку подолга од една минута, лут машки глас што наликува на гласот на Болсонару се расправа со некој што треба да биде неговиот син Едуарду, и се жали за тоа што го држат во болница. На снимката, мажот вели дека не може повеќе да го издржи „овој театар“, сугерирајќи дека се е режирано и одглумено.

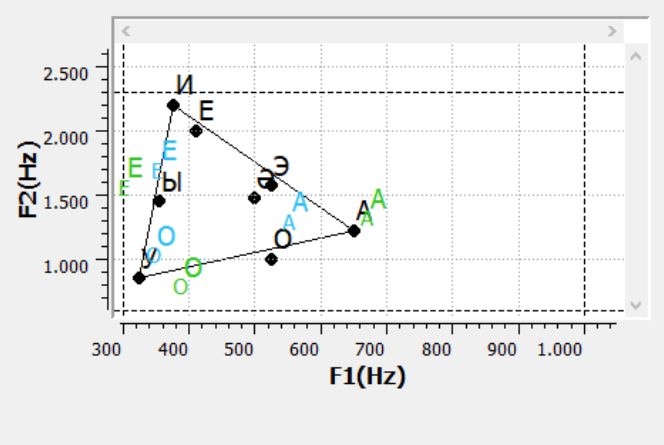
Истиот ден, Болсонару сè уште беше пациент на Одделението за полу-интензивна нега во болницата „Алберт Ајнштајн“ во Сао Паоло. Според медицинскиот извештај, немал повишена температура, се хранел интравенозно и ја повратил нормалната столица.

„Компрова“ не можеше да го пронајде оригиналниот извор на снимката. Снимката првенствено се шириле преку „ВотсАп“, во време кога документи можеа да се споделуваат во најмногу 20 конверзации. Тоа и овозможи да се шири со голема брзина и наскоро да премине и на другите социјални мрежи. Стана невозможно да се следи наназад до првиот извор. (Оттогаш, „ВотсАп“ го ограничи бројот на групи до кои може да се проследи една порака.)

Во неможност да го идентификува авторот (или авторите) на снимката, „Компрова“ се фокусираше на поконвенционална истрага и побара помош во експертиза од Бразилскиот Институт за форензички науки (Institute Brasileiro de Pericia). Експертите ја споредија виралната снимка со гласот на Болсонару од едно интервју од април 2018 година и заклучија дека гласот на снимката што се споделува на социјалните мрежи не е гласот на кандидатот.

Експертите направија квалитативна анализа на гласот, говорот и јазичните маркери на човекот што говори на снимката. Потоа ги споредија тие параметри за секој гласовен и говорен примерок. Во анализата, тие ги испитаа шемите на изговор на самогласките и согласките, ритамот и брзината на говорот, интонациските урнеци, квалитетот на гласот и навиките на говорникот, како и користењето на одредени зборови и граматички правила.

На пример, на следната слика е прикажана анализа на фреквенцијата на „формантите“, врвовите на амплитудите произведени од вибрациите на вокалниот тракт, шуплината во која се филтрира звукот произведен во грклanот. Воздухот во вокалниот тракт вибрира со различни амплитиди, во зависност од големината на трактот и обликот на отворот. Сликата ја прикажува анализата на фреквенцијата на формантите при изговор на самогласките „а“, „е“ и „о“. Самогласките обоени со зелено се од примерокот од аудио снимката што ја најдовме на „ВотсАп“, а сините самогласки се од примерокот од интервју со Болсонару неколку дена пред нападот врз него.



Дополнителна анализа утврди дека говорникот од снимката на „ВотсАп“ говори на начин што е типичен за руралните делови од државата Сао Паоло. А тоа го нема во говорниот стил на Болсонару. Во споредените примероци беа откриени разлики во резонанцата, артикулацијата, брзината на говорот и фонетските девијации.

„Компрова“ се консултираше и со друг експерт. Неговиот заклучок, исто така, беше дека гласот на снимката се различува од гласот на Болсонару во повеќе елементи. Кажа дека тонот на гласот изгледа малку поакутен од оној на Болсонару. Забележа и дека брзината на говорот е поголема од онаа на едно друго видео што кандидатот го снимил во болницата.

Друг елемент што го зацврсти заклучокот дека аудиото е фалсификат беше лошиот квалитет на снимката. Според искусните стручњаци, тоа е типичен трик што се користи за залажување: Намалувањето на резолуцијата на аудио и видео снимките и фотографи ја отежнува анализата.

Што се однесува до одговорот на Болсонару, неговите синови Флавиу и Карлос изјавија, во постови на социјалните медиуми, дека снимката претставува „лажна вест“.

Ако аудиото станеше вирално денес, веројатно ќе беше потешко да се поверува дека гласот е на Болсонару. Пред изборите, со само 18 секунди на телевизија дневно и пропуштање на изборните дебати поради хоспитализацијата и лекувањето, гласот на сегашниот претседател не беше толку познат. Тоа создаде можност фалсификуваната аудио снимка да измами многу луѓе.

Повеќе од една година подоцна, сè уште е тешко да се разбере зошто групи што го поддржуваа Болсонару и водеа кампања во негова полза ја споделија таа снимка која, ако се покажеше дека е автентична, можеше да ја уништи неговата кандидатура. Никогаш нема до крај да дознаеме зошто таквите групи ја споделуваа таа содржина со толку елан. Па сепак, таа служи како моќно потсетување дека содржина со експлозивни тврдења ќе се рашири по социјалните медиуми со голема брзина.

8. Истражување на интернет страници

Автор: Крег Силверман

Крег Силверман *(Craig Silverman) е медиумски уредник на BuzzFeed News, каде го предводи глобалниот тим за покривање на платформите, дезинформациите во онлајн сферата и медиумските манипулации. Тој претходно ги приреди „Прирачникот за верификација" и „Прирачникот за верификација за истражувачко новинарство", и е автор на „Лаги, проклети лаги и вирални содржини: Како информативните веб-страници шират (и раскринкуваат) онлајн гласини, непотврдени тврдења и погрешни информации" (Lies, Damn Lies, and Viral Content: How News Websites Spread (and Debunk) Online Rumors, Unverified Claims and Misinformation).*

Луѓето што се занимаваат со медиумски манипулации ги користат интернет страниците за да за-работат, да собираат адреси за електронска пошта и други лични информации, или да воспостават некаков онлајн градобран. Новинарите мораат да знаат како да го истражуваат присуството на интернет и, кога е можно, како да го поврзат со некоја поголема операција што може да вклучува сметки на социјалните медиуми, аппликации, трговски друштва или други субјекти.

Запомнете дека текстот, сликите или целата интернет страница може да исчезне со текот на времето - особено ако почнете да ги контактирате и да поставувате прашања. Најдобра пракса е да се искористи „Вејбек Машин" (Wayback Machine) за зачувување на значајните страници на таргетираниот веб-сајт како дел од вашата редовна работа. Ако таму не можете соодветно да ја снимите страницата, користете алатка како што е archive.today. Тоа обезбедува можност да поставувате линкови до архивирани страници како доказ што ќе ги поткрепи вашите наоди, и да избегнете линкување директно до страница што шири мисинформации и дезинформации. („Ханчли" (Hunchly) е одлична платена алатка за создавање на лична архива на интернет-страници, автоматски, додека работите.) Овие алатки за архивирање се од огромно значење во истражувањето како се менувал изгледот на некоја интернет страница низ нејзината историја. Препорачува и да го инсталирате додатокот за прелистувачи на „Вејбек машин" за полесно да ги архивирате страниците и да ги прегледувате нивните претходни верзии.

„Гоустери" (Ghostery) е уште еден корисен додаток за прелистувачи, кој ќе ви ги прикаже „тракерите" што се присутни на некоја интернет страница. Тоа ќе ви помогне брзо да идентификувате дали страницата користи „Гугл Аналитикс" (Google Analytics) и/или „Гугл Адсенс" (Google AdSense) идентификациски кодови, што ќе ви помогне во користењето на една од техниките наведени подолу.

Ова поглавје ќе разгледа четири категории за анализа кога се истражува некоја интернет страница: Содржината, кодот, аналитиката, регистрацијата и со неа поврзаните елементи.

Содржина

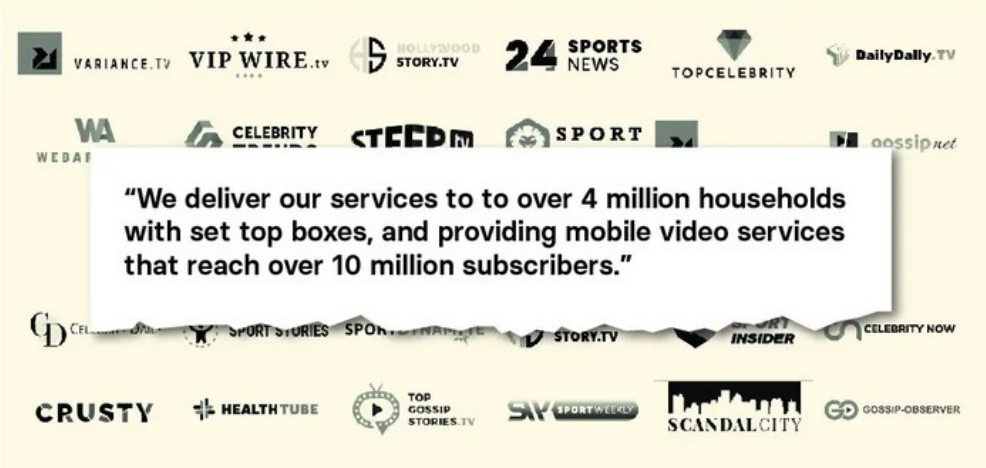
Најголемиот број интернет страници ви кажуваат барем малку за тоа кои се и што се. Без оглед дали се работи за посебна страница „За нас“ (About), опис на дното на страницата или на друго место, тоа е добро место да ја почнете истрагата. Истовремено, недостиг на јасни информации може да биде знак дека интернет-страната е креирана набрзина, или се обидува да прикрие детали за нејзината сопственост или цел.

Заедно со читањето на основниот текст „За нас“, извршете детален преглед на содржината на интернет страната, со цел да утврдите кој раководи со неа, која е нејзината цел и дали е дел од некоја поголема мрежа или иницијатива. Некои работи на кои треба да внимавате:

- Дали е идентификуван сопственикот или каков било корпоративен субјект на страницата „За нас“? Исто така, забележете ако нема страница „За нас“.
- Дали наведува некое трговско друштво или лице во белешката за авторското право на дното на насловната или на некоја друга страница? Дали наведува какви било имиња, адреси или корпоративни субјекти во политиката за приватност или во условите за користење? Дали тие имиња или трговски друштва се различни од оние наведни во „футерот“, на страницата „За нас“ или на други локации на интернет страната?
- Ако објавува информативни статии, забележете ги авторите и дали тие белешки содржат активни линкови на кои може да се клика. Ако содржат, проверете дали водат до страница со повеќе информации за авторите, како што се биографија или линкови до сметките на социјалните мрежи на авторот.
- Дали на интернет страната се поставени поврзаните сметки на социјалните мрежи? Можат да бидат во форма на мали икони на врвот, дното или на маргините на насловната страница, или „вградени“ со покана да ја „лајкувате“ нивната страница на Фејсбук, на пример. Ако страната прикажува икони за платформи како што се Фејсбук и Твитер, поминете со глувчето преку нив и погледнете во долниот лев агол на прелистувачот за да видите до која УРЛ адреса водат. Често се случува набрзина подготвена интернет страница да пропушти да ги пополни специфичните идентификациски броеви на социјалните профили. Во таков случај, ќе видите дека линкот гласи само facebook.com/ без корисничко име.
- Дали интернет страната наведува некакви производи, клиенти, сведоштва или други лица или трговски друштва со кои можеби е поврзана и кои би вредело да се проверат?
- Осигурајте се дека проверката нема да се задржи само на насловната страница. Кликнете на сите главни менија и прегледајте ги сите опции за да пронајдете други страници што треба да ги посетите.

Значаен сегмент од прегледувањето на содржината е утврдувањето дали се работи за оригинална содржина. Дали текстот на страницата „За нас“ или други општи текстови на интернет страната се копирани од некаде? Дали интернет страната шири лажни или заведливи информации, или турка одредена агенда?

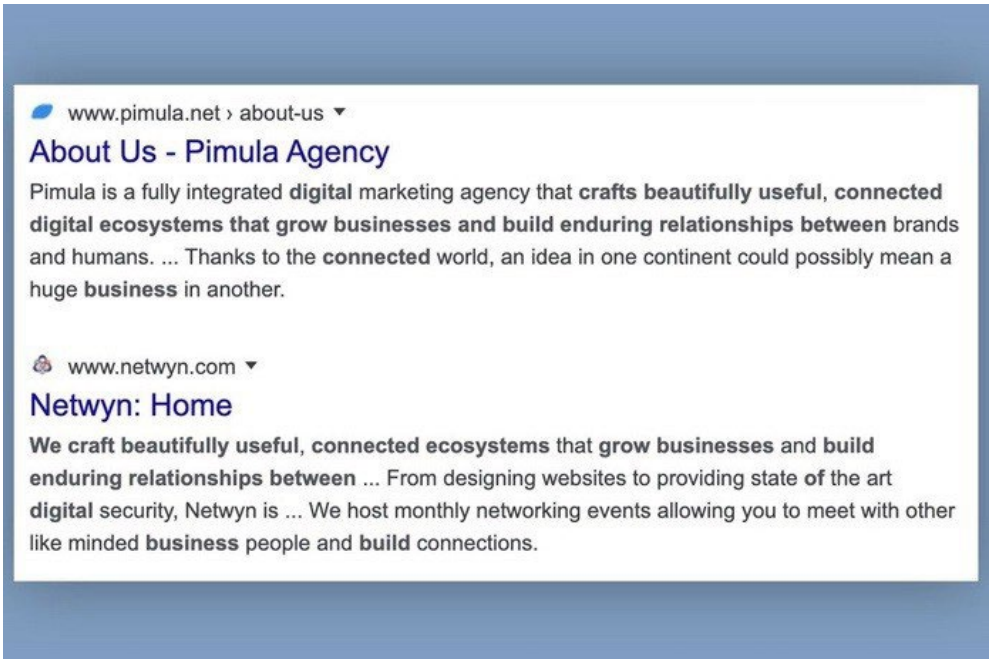
Во 2018 година истражував голема измамничка шема за дигитално огласување што вклучуваќе мобилни апликации и интернет страници, фиктивни компании, непостоечки вработени во непостоечки компании. На крај открив повеќе од 35 интернет страници поврзани со шемата. Еден од начините на кој ги идентификував тие страници беше со копирање на текстот на страницата „За нас“ на една од интернет-страните и пребарување на тој текст на Гугл. Веднаш пронајдов околу 20 интернет страници со идентичен текст:



Измамниците што ја водеа шемата исто така создадоа интернет-страници за нивните фиктивни компании за да изгледаат како легитимни субјекти кога потенцијалните партнери од мрежите за огласување ќе ги посетат за да ги направат потребните проверки. Еден пример за тоа е компанијата со име „Атосес“ (Atoses). На нејзината интернет страница беа наведени неколку вработени со портретни фотографии. Реверзибилното пребарување на слики на Јандекс (Yandex) (најдобриот пребарувач на слики за портретни фотографии) набрзина откри дека неколку од нив се „сток“ фотографии:

„Атосес“ исто така го имаше следниот текст во „футерот“ на интернет страната: „Изработуваме прекрасни и корисни, поврзани екосистеми што помагаат во растежот на бизнисите и градат трајни врски помеѓу онлајн медиумите и корисниците“.

Истиот текст се појавува на интернет страните на најмалку две маркетинг-агенции:



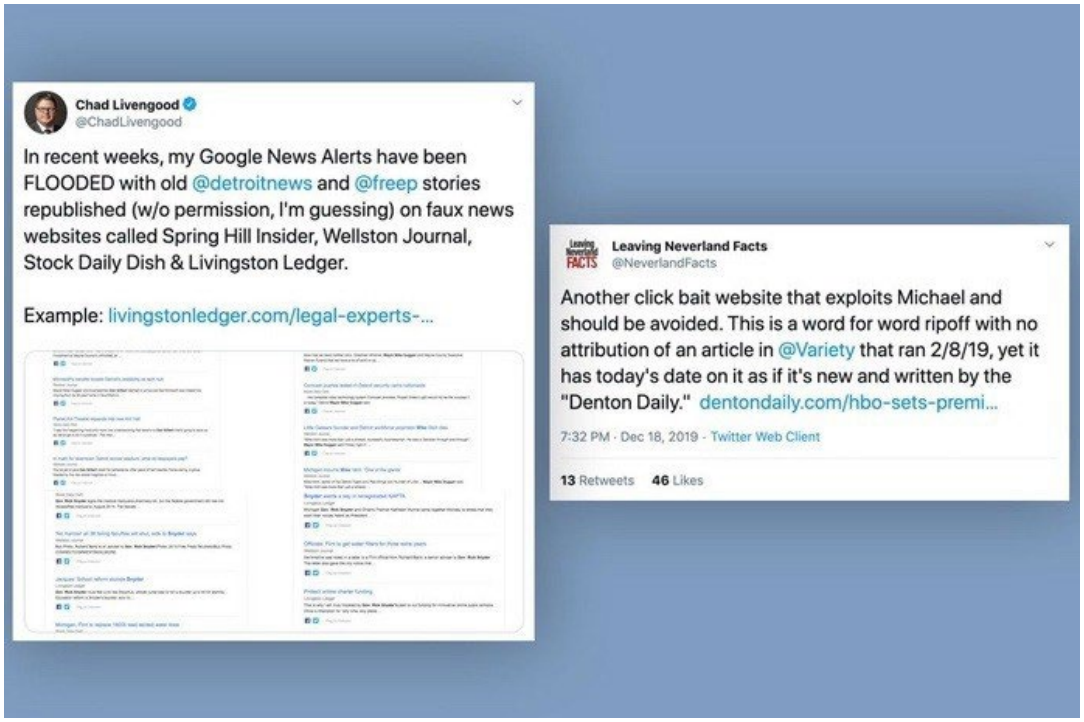
Ако компанијата користи „сток“ фотографии како слики на своите вработени и плагиран текст на својата интернет страница, знаете дека не е тоа за што се претставува.

Подеднакво добра идеја е да копирате делови од статиите објавени на интернет страната и да ги внесете во пребарувачот на Гугл или во друг пребарувач. Понекогаш, интернет страна што тврди дека е извор на вести само плагира вистински медиумски организации.

Во 2019 година, налетав на една интернет страна со име forbesbusinessinsider.dom што изгледаше како информативна интернет-страница што ја покрива технолошката индустрија. Во реалност, таа се занимаваше со масовно плагирање на статии од многу медиуми, вклучувајќи, што навистина е смешно, и една моја статија за лажните локални интернет страници.

Друг основен чекор е пребарувањето на УРЛ адресата на интернет страната во Гугл. На пример, “forbesbusinessinsider.com.” Така ќе добиете увид колку од нејзините страници се индексирани, а можеби и примери за други луѓе што известувале за неа или ја спомнале на некој друг начин. Можете да проверите и дали интернет страната е излистана на Гугл Њус (Google News) со отворање на насловната страница на Гугл Њус и внесување на „forbesbusinessinsider.com“ во полето за пребарување.

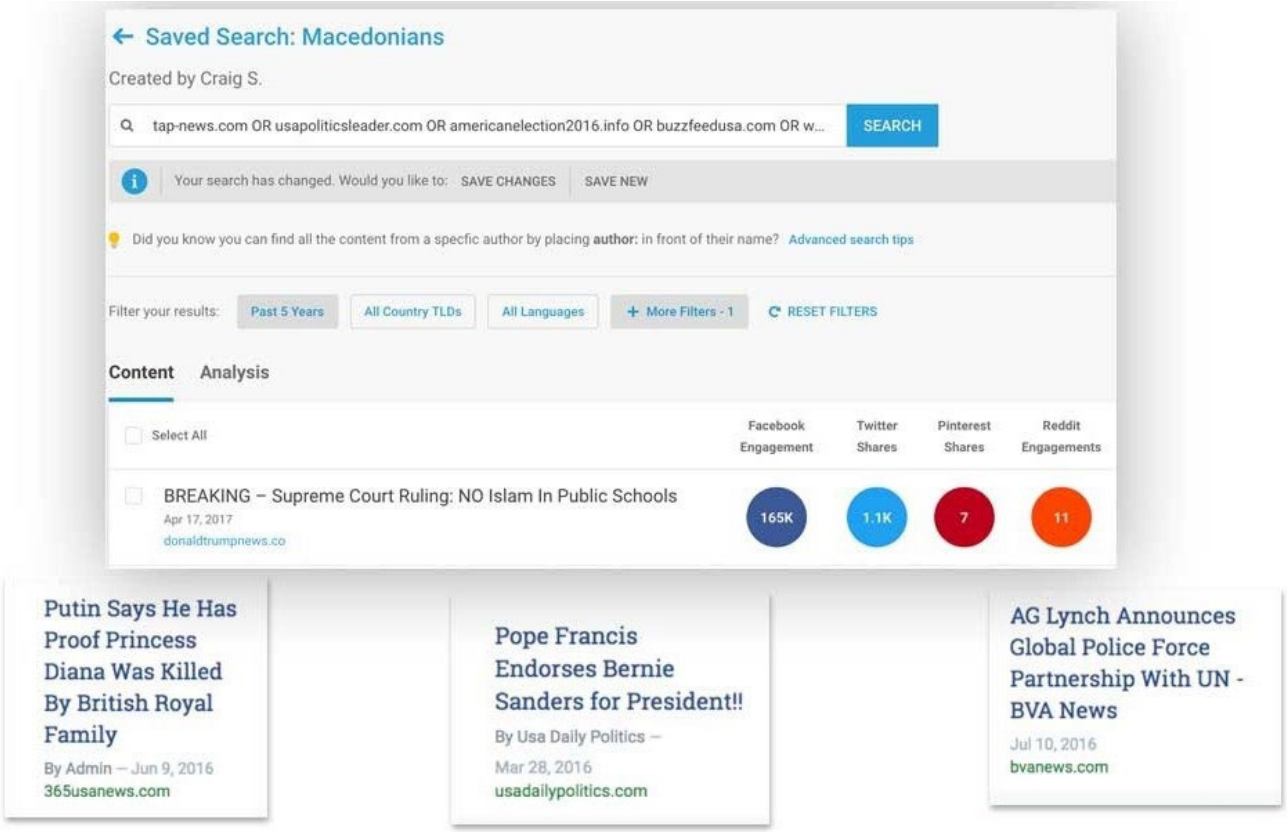
Друг корисен совет е УРЛ адресата да ја внесете во полињата за пребарување на Twitter.com или Facebook.com. Резултатите ќе ви покажат дали луѓето поставуваат линкови до таа интернет страница. Во една истрага, налетав на интернет страницата dentondaily.com. Насловната страница прикажуваше само неколку статии објавени на почетокот на 2020 година, а кога го пребарав името на доменот на Твитер, дознав дека претходно таа „пумпала“ плагирани содржини што предизвикале луѓето да го забележат тоа и да се пожалат. Тие постари статии беа избришани од страната, но твитовите обезбедуваа докази за начинот на кој претходно се однесувала.



Откако ќе ја пронајдете содржината, време е да почнеме да разбираме како таа се шири. Ќе разгледаме две алатки што ќе ни помогнат со таа задача: „БазСумо“ (BuzzSumo) и „КраудТенгл“ (CrowdTangle).

Во 2016 година, со истражувачот Лоренс Александер (Lawrence Alexander) ги истражувавме информативните интернет страници фокусирани на американската политика управувани од странство. Наскоро наидовме на интернет страници што функционираа во Велес, град во Северна Македонија. Со помош на информациите за регистрација на домени (повеќе за тоа подолу во текстов) идентификувавме повеќе од 100 интернет страници посветени на политиката во САД што функционираа во тој град. Сакав да видам колку популарни се нивните содржини и каков вид на статии објавуваат. Ги земав УРЛ адресите на неколкуте интернет страници што изгледаа најактивни и извршив пребарување во „БазСумо“ (BuzzSumo), алатка што ги рангира содржините на некоја интернет страница врз основа на ангажманот што го предизвикале на Фејсбук, Твитер, Пинтерест (Pinterest) и Редит. (Постои и бесплатна верзија, иако платената верзија дава многу повеќе резултати.)

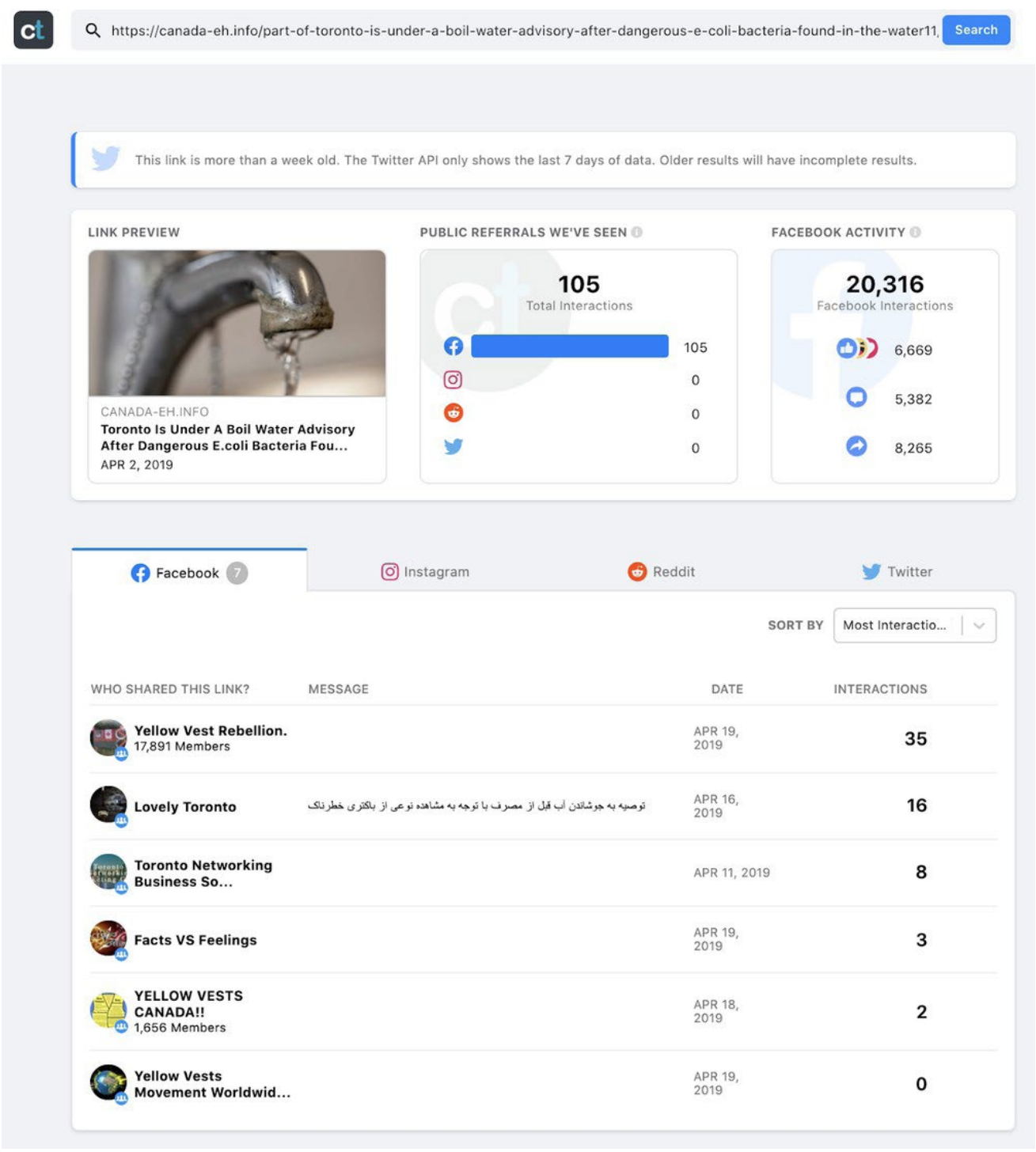
Веднаш увидов дека статиите на тие интернет страници што имаа најголем ангажман на Фејсбук беа целосно лажни. Тоа ни обезбеди клучни информации и агол на гледање што се разликуваше од претходно објавените извештаи за таа тема. На следната слика е прикажан екранот со резултатите од основно пребарување на БазСумо, со наведување на ангажманот за одредена интернет-страница на Фејсбук, Твитер, Пинтерест и Редит, како и примери од лажните приказни од 2016 година:



Друг начин да идентификуваме како содржината на некоја интернет страница се шири на Фејсбук, Твитер, Инстаграм и Редит е да го инсталираме бесплатниот додаток за прелистувачи „КраудТенгл“ или да ја искористиме неговата онлајн алатка за пребарување линкови. Двете ги нудат истите функционалности, но во нашиот пример ќе работиме со онлајн верзијата. (Иако алатките се бесплатни за користење, за пристап ви е потребна корисничка сметка на Фејсбук.)

Клучната разлика помеѓу „БазСумо“ и „КраудТенгл“ е што во првиот можете да внесете УРЛ адреса од саканата интернет страна и тој веднаш ќе ви прикаже која содржина од страната предизвикала најголем ангажман. „КраудТенгл“ се користи за проверка на специфична УРЛ адреса од некоја интернет страна. Ако, на пример, во „КроудТенгл“ ја внесете адресата buzzfeednews.com, ќе ви ги прикаже статистиките за ангажманот само за насловната страна, додека „БазСумо“ ќе ги скенира сите содржини на целиот домен за да ги идентификува содржините со најголем ангажман. Друга разлика е што алатката за пребарување на линкови и додатокот за прелистувачи на „КраудТенгл“ ќе ви го прикаже ангажманот на Твитер само за последните седум денови. „БазСумо“ ги пребројува сите споделувања на статии од интернет страната на Твитер од моментот на објавувањето.

На пример, ја внесов УРЛ адресата на една стара, лажна приказна за задолжително превривање на водата од Торонто во пребарувачот на линкови на „КраудТенгл“ (CrowdTangle Link Search). (Интернет страната подоцна ја избриша статијата, но УРЛ адресата беше сè уште активна во моментот на пишување на овие редови). „КраудТенгл“ покажува дека таа УРЛ адреса добила повеќе од 20,000 реакции, коментари и споделувања на Фејсбук од моментот на објавувањето. Исто така ги прикажува некои од страниците и јавните групи што го споделиле тој линк, а нуди и опција да ги видите тие податоци за Инстаграм, Редит и Твитер. Запомнете: Јазичето за Твитер ќе ги прикаже само твитовите од претходните седум денови.



Забележете дека високиот вкупен број на интеракции на Фејсбук не е вистински одразен на кратката листа на страници групи што ја гледаме. Тоа делумно се должи на фактот што Фејсбук подоцна отстрани некои од клучните страници што го шириа ликнот кога беше објавен за прв пат. Ова е корисен потсетник дека „КраудТенгл“ ги прикажува само податоците од активни сметки и нема да ја прикаже баш секоја јавна сметка што споделила некоја УРЛ адреса. Се работи за избор, па сепак, неверојатно корисен избор затоа што често открива јасна врска помеѓу одредени сметки на социјалните медиуми и некоја интернет страна. Ако истата Фејсбук страница конзистентно - или исклучиво - споделува содржини од некоја интернет страна, тоа може да е знак дека со нив раководат истите луѓе. Сега можете да навлезете подлабоко во страницата и да ги споредите информациите со интернет страната, а потенцијално и да ги идентификувате инволвираните лица и нивната мотивација. Некои резултати од пребарување на линкови на Фејсбук прикажани во „КраудТенгл“ можат да бидат од луѓе што ја споделуваат статијата во група на Фејсбук. Забележете ја сметката што го споделила линкот и проверете дали ширела и други содржини од таа интернет страна. Повторно, можеби има некаква поврзаност.

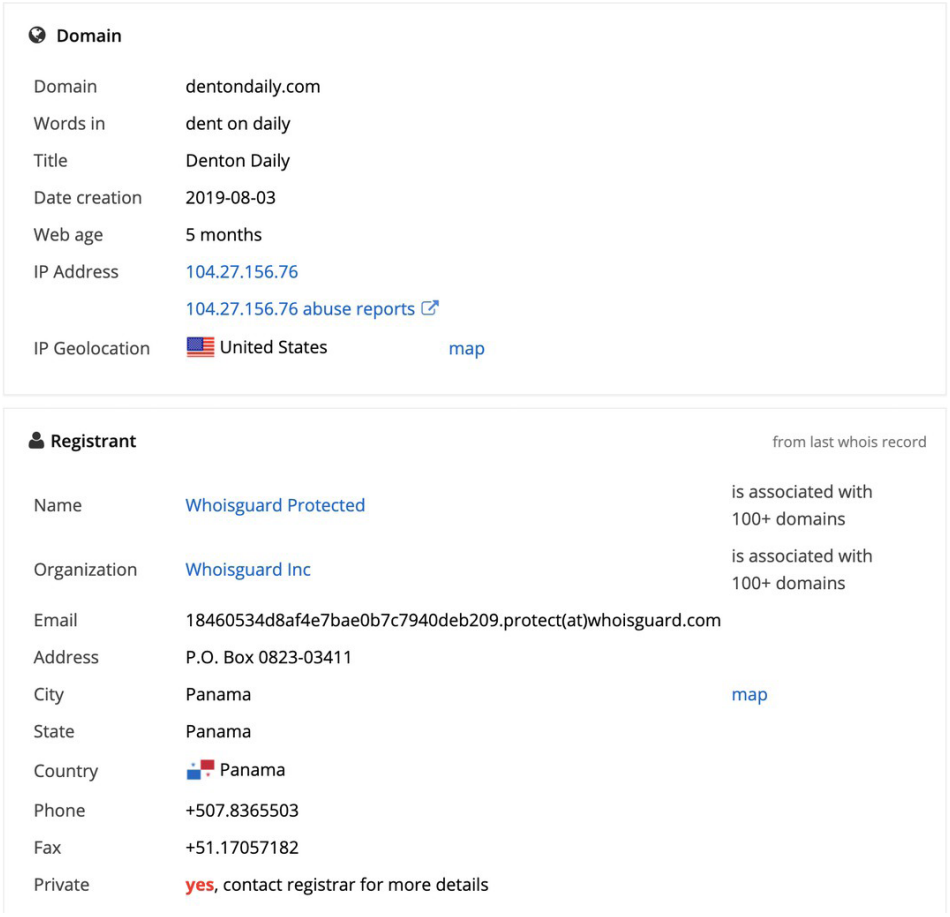
Регистрација

Секое име на домен на интернет е дел од централна база на податоци што ги чува основните информации за создавањето и историјата на доменот. Во некои случаи може да ни се посреќи и да пронајдеме информации за лицето или субјектот што платило за регистрацијата на некој домен. Тие информации можеме да ги извлечеме со пребарување „whois“ („кој е“) што го нудат повеќе бесплатни алатки. Постојат и грст одлични бесплатни и ефтини алатки што можат да понудат дополнителни информации, како што е историјатот на сопственоста на некој домен, серверите на кои бил хостиран и други корисни детали.

Една задршка се однесува на релативно ефтината опција за плаќање за заштита на приватноста на вашите лични податоци кога регистрирате домен. Ако спроведете „whois“ пребарување за некој домен и резултатите прикажат нешто од следниве, „Реџистрејшн прајват“ (Registration Private), „ХуисГард Протектед“ (WhoisGuard Protected), или „Перфект прајваси ЛЛЦ“ (Perfect Privacy LLC) како регистрант, тоа значи дека имаат заштита на приватноста.
Дури и во таквите случаи, пребарување „whois“ ќе ни го даде датумот на последната регистрација на доменот, кога истекува регистрацијата, и АјПи адресата на интернет на која е хостирана интернет страната.

DomainBigData е една од најдобрите бесплатни алатки за истражување на имиња на домени и нивниот историјат. Можете, наместо да пребарувате со УРЛ адреса, да внесете е-маил адреса или име на лице или компанија. Други ефтини услуги што можеби ќе посакате да ги забележите се DNSLytics, Security Trails и Whoisology. Одлична но поскапа опција е истражувачката алатка „Ирис“ (Iris) на „ДомејнТулс“ (DomainTools).

На пример, ако во „ДомејнБигДата“ (DomainBigData) ја внесеме адресата dentondaily.com, ќе видиме дека има заштита на приватноста. Името на регистрантот е наведено како „Whoisguard Protected“. За среќа, сè уште можеме да видиме дека последната регистрација е од август 2019 година.



Domain

Domain	dentondaily.com
Words in	dent on daily
Title	Denton Daily
Date creation	2019-08-03
Web age	5 months
IP Address	104.27.156.76
	104.27.156.76 abuse reports
IP Geolocation	United States map

Registrant from last whois record

Name	Whoisguard Protected	is associated with 100+ domains
Organization	Whoisguard Inc	is associated with 100+ domains
Email	18460534d8af4e7bae0b7c7940deb209.protect(at)whoisguard.com	
Address	P.O. Box 0823-03411	
City	Panama	map
State	Panama	
Country	Panama	
Phone	+507.8365503	
Fax	+51.17057182	
Private	yes, contact registrar for more details	

За споредба со друг пример, пребарајте го newsweek.com во „ДомејнБигДата“ (DomainBigData). Веднаш гледаме дека сопственикот не платил за заштита на приватноста. Наведени се името на компанијата, е-маил адреса, телефонски број и телефакс.

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	

Исто така гледаме дека тој субјект го поседува доменот од мај 1994 година и дека интернет страната во моментов е хостирана на АјПи adresa 52.201.10.13.Следна работа што треба да се забележи е дека името на компанијата, е-маил адресата и АјПи адресата се потцртани како линкови. Тоа значи дека можат да не одведат до другите домени што и припаѓаат на компанијата „Њузвик ЛЛЦ“ (Newsweek LLC), domains@ibtimes.com и други интернет страни хостирани на таа АјПи адреса. Таквите врски се неверојатно значајни за истрагата, така што секогаш е важно да ги разгледаме другите домени што ги поседува тоа лице или субјект.

За АјПи адресите, имајте на ум дека целосно неповрзани интернет страни можат да бидат хостирани на ист сервер. Тоа вообичаено се случува затоа што луѓето користат иста хостинг компанија за своите интернет страни. Општо правило е дека што помалку интернет страни се хостирани на ист сервер, толку поголема е веројатноста дека тие се меѓусебно поврзани. Секако, не можете да бидете сигурни дека е така.

Ако гледате стотици интернет страни хостирани на еден сервер, можеби нема никаква поврзаност на нивната сопственост. Но ако видите само девет страни, на пример, а едната за која сте заинтересирани има заштита на приватноста на податоците за регистрација, вреди да се направи пребарување „whois“ за другите осум домени за да видите дали можеби имаат ист сопственик и дали е можно тоа лице да е сопственик на интернет страната што ја истражувате. Луѓето може да платат за заштита на приватноста на некои домени, но да пропуштат тоа да го направат за други домени.

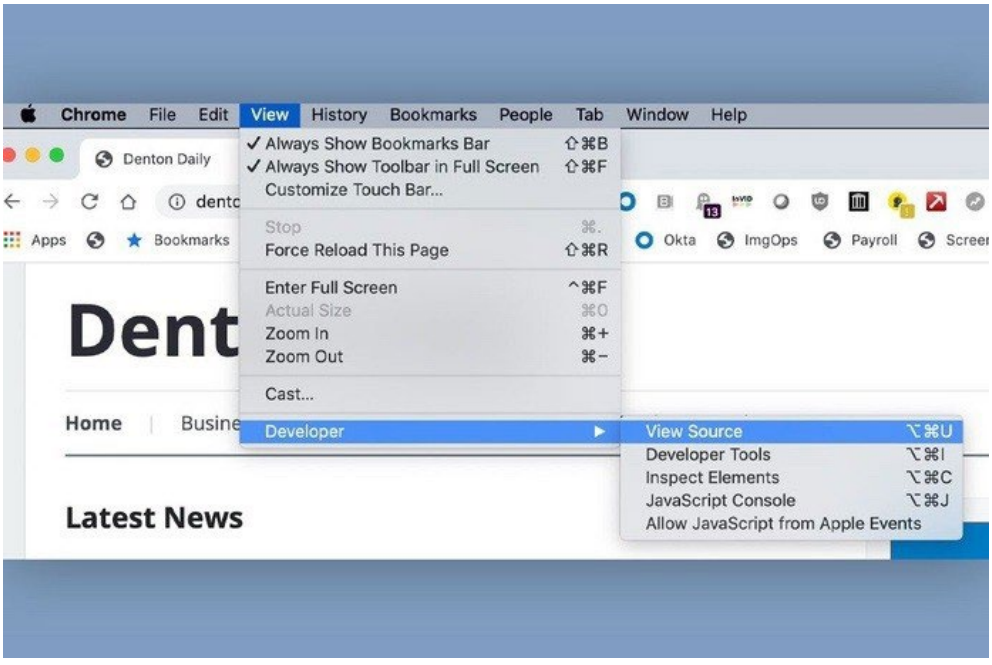
Поврзувањето на интернет страните преку нивните АјПи адреси, содржина и/или податоци за регистрацијата е основен начин за идентификација на мрежи и актерите што стојат зад нив.

Сега да погледнеме еден друг начин за поврзување на интернет страните со користење на програмскиот код.

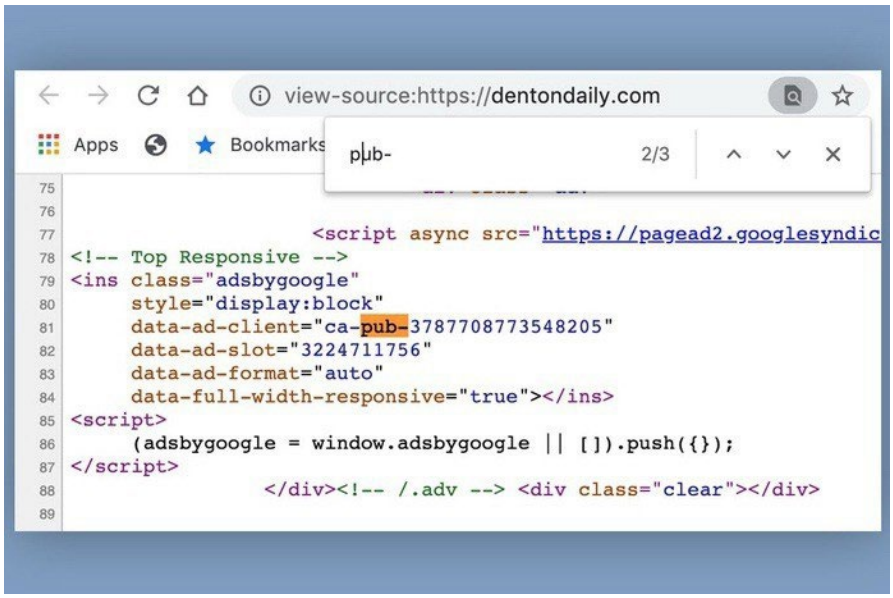
Програмски код и аналитика

Овој приод, откриен од Лоренс Александер (Lawrence Alexander), почнува со преглед на изворниот код на интернет страната и пребарување во него за да се види дали тој ги содржи кодовите на Гугл Аналитикс (Google Analytics) и/или Гугл АдСенс (Google AdSense). Се работи за мошне популарни производи на Гугл што, соодветно, му овозможуваат на сопственикот на страната да ги следи статистиките на страната или да заработи од продажба на рекламен простор. По интеграцијата на интернет-страната, секоја страница ќе добие единствен идентификациски код поврзан со сметката на Гугл Аналитикс или АдСенс на сопственикот. Кога некој води повеќе интернет страни, често се користат истите сметки за „Аналитикс“ и „АдСенс“ за управување со тие страни. Тоа на истражувачот му дава можност да поврзе навидум неповрзани интернет страни со пронаоѓање на истиот идентификатор во изворниот код. За среќа, тоа е лесно да се направи.

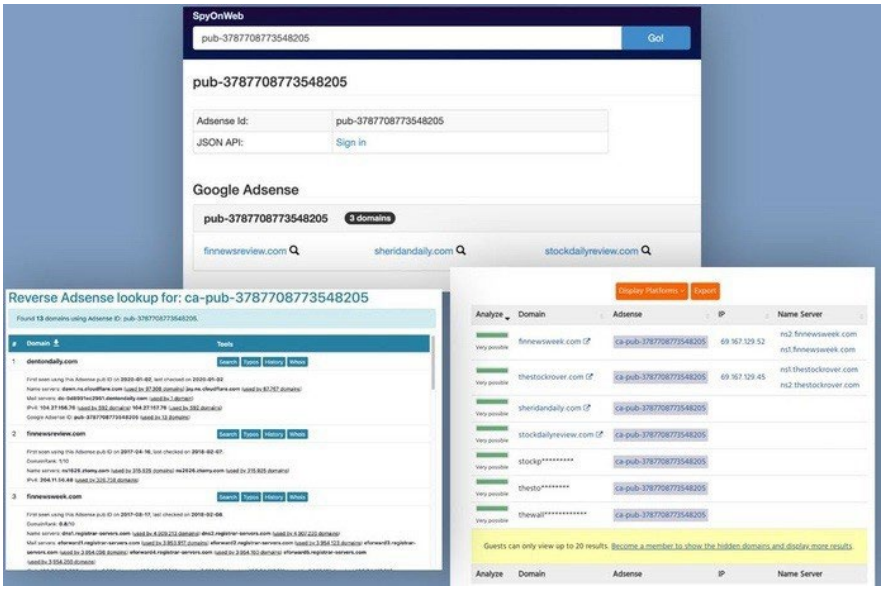
Прво одете на целната интернет страна. Во нашиот пример тоа е dentondaily.com. Во прелистувачот „Хром“ за Макинтош, изберете го менито „View“, а потоа „Developer“ па „View Source“. Тоа отвора ново јазиче со изворниот код на страната. (На „Хром“ за персонален компјутер (PC), притиснете ctrl-U.)



Сите идентификатори на Гугл Аналитикс почнуваат со „ua-“ следено од низа цифри. Идентификаторите на АдСенс почнуваат со „pub-“ следено од низа цифри. Можете да ги лоцирате во изворниот код со користењето на функцијата „find“ на интернет страната. На Мак (Mac) сметачи, внесете „command-F“; на ПЦ „ctrl-F“. Се отвара мало поле за пребарување. Внесете “ua-” или “pub-” и ќе ги видите сите идентификатори во страната.



Ако пронајдете идентификатор, копирајте го и внесете го во полето за пребарување на сервиси како што се SpyOnWeb, DNSlytics, NerdyData или AnalyzeID. Треба да се знае дека често ќе добиете различни резултати на различни сервиси, затоа е важно да го тестирате идентификаторот и да ги споредите резултатите. На следната слика можете да видите дека „СпајОнВеб“ (SpyOnWeb) пронајде три домени со ист АдСенс идентификатор, но „ДНСЛитикс„ (DNSLytics) и „АналајзИД“ (AnalyzeID) пронајдоа неколку домени повеќе.



Понекогаш се случува интернет страната да имала идентификатор во минатото, но веќе го нема. Затоа е од огромно значење да се користи истиот приод за преглед на изворот на сите други наведени интернет страни што наводно ги имаат индикаторите за да се потврди нивното присуство. Треба да знаете дека идентификаторите на АдСенс и Аналитикс сè уште се присутни во архивираната верзија на интернет страната во „Вејбек машин“ (Way-back Machine). Значи, ако не пронајдете идентификатор на некоја активна интернет-страна, задолжително проверете ја на „Вејбек машин“.

Сите спомнати сервиси ги даваат некои од резултатите бесплатно. Често е потребно да се плати за да се добијат сите резултати, особено ако бараниот идентификатор е присутен на голем број други интернет страни.

Една завршна забелешка за проверката на изворниот код: Добро е да се скенира целата страница, дури и ако немате познавање од „HTML“, „JavaScript“, „PHP“ или друг популарен програмски јазик за интернет. На пример, луѓето понекогаш забораваат да го сменат името на страницата или на интернет страната ако го користат истиот дизајнерски образец. Таков едноставен пропуст може да понуди точка за поврзување.

Кога ја истражував шемата за имами со реклами со фиктивни компании како „Атосес“, се заинтересирав за една компанија со име „Флај апс“ (FLY Apps). Го проверив изворниот код на нивната интернет-страна со само една страница и на почетокот од изворниот код го видов зборот „Loocrum“ како обичен текст:

```
<input type="submit" name="submit" value="" style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; color:inherit;font:inherit;font-family:inherit;font-size:inherit;line-height:inherit;-webkit-appearance:button;cursor:pointer;background-image:url('https://archive.is/lG6hf/de442e0343d248b28ace0397c40e6769735eeaf8.svg');background-color: transparent; width:18px;height:14px;text-indent:-9999px;background-repeat: no-repeat; border-width: medium; border-style: none; margin: 0px; border-color: white; "/>
<span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
</div>
<span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
</form>
<span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
</div>
<span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; display:table;clear:both;"> </span></div>
<span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; display:table;clear:both;"> </span></div>
<div style="text-align:left;box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; background-color: rgb(141, 118, 190); position:absolute;top:0px;right:0px;bottom:0px;left:0px;z-index:5;display:none;"><span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
<div style="text-align:left;box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; margin-right:auto;margin-left:auto;padding-left:15px;padding-right:15px;"><span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; display:table;"> </span>
<span style="text-align:left;box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; float:left;line-height:20px;font-family:ralewayblack, sans-serif;font-size:29px;text-transform:uppercase;height:auto;margin-left:15px;margin-top:9px;color:rgb(255, 255, 255);padding: 3px 15px; "><span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; ">
</span>Loocrum<span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span></span>
<div style="text-align:left;box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; float:right;margin: 24px 5px 0px 0px; "><span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
```

Пребарувањето на тој збор на Гугл прикажа компанија по име „Лукрум“ (Loocrum) што користеше потполно исто дизајнерско решение за интернет страната како „Флај Апс“ а делумно имаше и иста содржина. „Whois“ пребарување откри дека е-маил адресата користена за регистрација на доменот loocrum.com била користена за регистрација на други фиктивни компании што претходно ги идентификував како делови од шемата. Врската помеѓу „Флај Апс“ и „Лукрум“ обезбеди значајни дополнителни докази дека четворицата луѓе што раководат со „Флај Апс“ се поврзани со целата шема. Сето тоа беше откриено со едноставен преглед на изворниот код и барање на обичен текст што изгледаше како да не му е таму местото.

Заклучок

Дури и ако ги имате на располагање сите наведени приоди и алатки, понекогаш можете да се чувствувате како да сте наишлче на ќор-сокак. Често постојат други начини да ги откриете врските или патеките за натамошно истражување на некоја интернет страна. Кликнете на сите линкови, проучете ја содржината, прочитајте го изворниот код, видете кој е потпишан на интернет-страната, кој ги споделува содржините, и проверете сè друго што може да ви падне на ум за да откриете што всушност се случува.

9. Анализа на рекламите на социјалните мрежи

Автор: Џоана Вајлд

Џоана Вајлд *(Johanna Wild) е истражувач на отворени извори во „Белингкет" и е фокусирана на развој на технологии и алатки за дигитални истражувања. Има претходно искуство во онлајн новинарството, а пред тоа има работено со новинари во (пост)конфликтни региони.*
Една од нејзините улоги беше да дава поддршка на новинари од Источна Африка во производството на емисии за „Гласот на Америка" (Voice of America).

Рекламите што ги гледате на хронолошкиот преглед на вашите социјални медиуми не се исти со рекламите што луѓето што седат до вас во градскиот транспорт ги гледаат на нивните социјални медиуми. На основа на различни фактори, како што се вашата локација, род, возраст и тоа што сте означиле дека ви се допаднало или сте споделиле на мрежата, можеби ќе ви прикажат реклами за луксузни апартмани за одмор во Малага, додека вашиот сосед гледа реклами за јапонски игри за мобилен телефон.

Микротаргетирањето, категоризацијата на корисниците во целни групи за да им се прикажат реклами што одговараат на нивните животни околности и интереси, станаа причина за голема загриженост во време на избори. Загриженоста е околу можноста дека кампањите можат да таргетираат сосема мали делови од населението со реклами што ги подгреваат нивните стравови или омраза, или такви што шират лажни информации. Општо земено, рекламите на политичарите поставени на социјалните мрежи не се предмет на проверка на факти. Фејсбук, на пример, во јануари 2020 година потврди дека ќе продолжи да дозволува секакви политички реклами доколку се придржуваат до стандардите на заедницата на Фејсбук. Тоа значи дека специфични групи корисници можат да бидат таргетирани со реклами што содржат дезинформации за клучни политички или општествени теми.

До неодамна, беше скоро невозможно новинарите и истражувачите да добијат увид во рекламите наменети за различни корисници. Како одговор на јавната критика за недостигот на транспарентност, неколку социјални мрежи создадоа библиотеки на реклами што овозможуваат секој што тоа го сака да ги прегледа информациите за рекламите објавени на нивните платформи.

Токму библиотеката на Фејсбук беше обвинета дека не ги прикажува веродостојно сите достапни реклами. Значи, секогаш кога ги користите таквите библиотеки, треба да посветите одредено време да проверите дали сите реклами што се појавиле на вашиот хронолошки приказ можат да се пронајдат во библиотеката.

Библиотеките на реклами сепак се значаен чекор напред кон поголема транспарентност и им нудат на новинарите и на други лица возбудливи нови начини за проучување на дигиталното рекламирање. Следните техники ќе ви помогнат да започнете со истражување на рекламите поставени на водечките платформи како што се Гугл, Твитер и Фејсбук.

Гугл

Центарот за реклами на Гугл е добро скриен во нивниот Извештај за транспарентноста (Transparency Report). Искористете го овој линк за пристап до одделот за политичко рекламирање кој дава информации за рекламите на Гугл и Јутјуб наречани од Европската Унија, Индија и САД.

Страниците посветени на секој од тие региони прикажуваат списоци од држави и вкупните трошења за рекламирање од моментот на објавување на извештајот (како што е прикажано на следната слика).

Ad spend per geography

Country	Ad spend
Austria	€930,850
Belgium	€392,150
Bulgaria	€10,900
Croatia	€94,150
Cyprus	€6,200
Czechia	€49,550
Denmark	€570,650
Estonia	€21,450
Finland	€206,000
France	€12,850

‹ PREVIOUS 1 of 3 NEXT ›

Кликнете на името на државата и ќе стигнете на страница што ја содржи базата на податоци на реклами од таа држава:

View ads

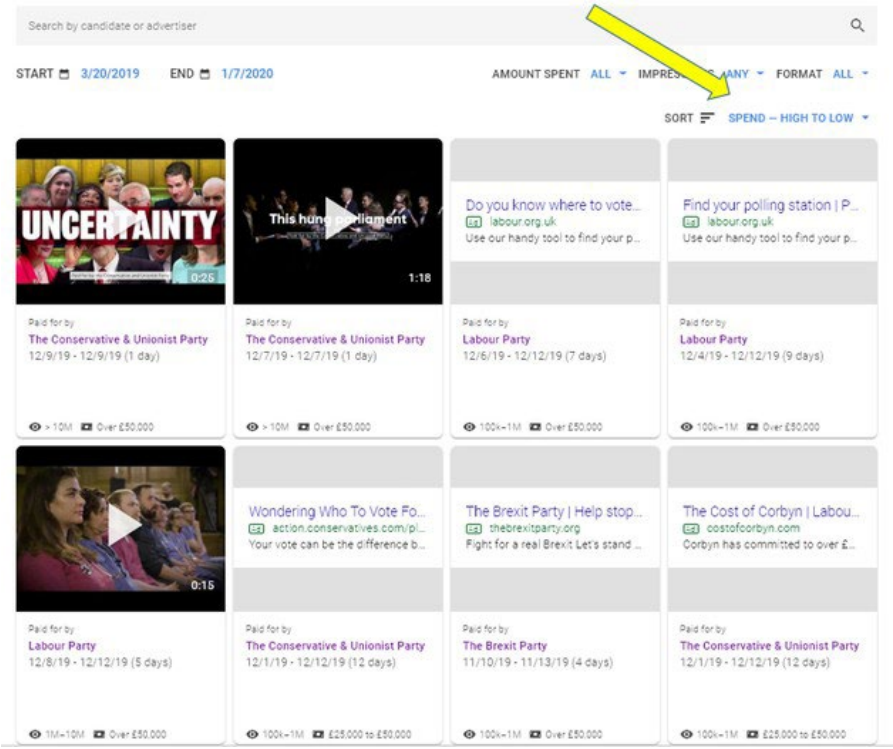
Search by candidate or advertiser

START 3/20/2019 END 1/7/2020 AMOUNT SPENT ALL IMPRESSIONS ANY FORMAT ALL

SORT MOST RECENT

Резултатите можете да ги филтрирате по датум, сумата на потрошени пари и бројот на прикажувања на рекламата на корисниците (импресии). Можете да филтрирате и по форматот на рекламата ако сакате да ги видите резултатите за видео, сликовни или текстуални реклами.

Исто така, лесно е да се издвојат оние што потрошиле најмногу пари на рекламирање. На пример, ако сакате да ги видите најголемите политички рекламни кампањи од Велика Британија од моментот на објавување на извештајот до јануари 2020 година, едноставно во категоријата „sort“ (подреди) изберете „spend - high to low“ (трошења - од најголеми кон најмали), како што е прикажано подолу.

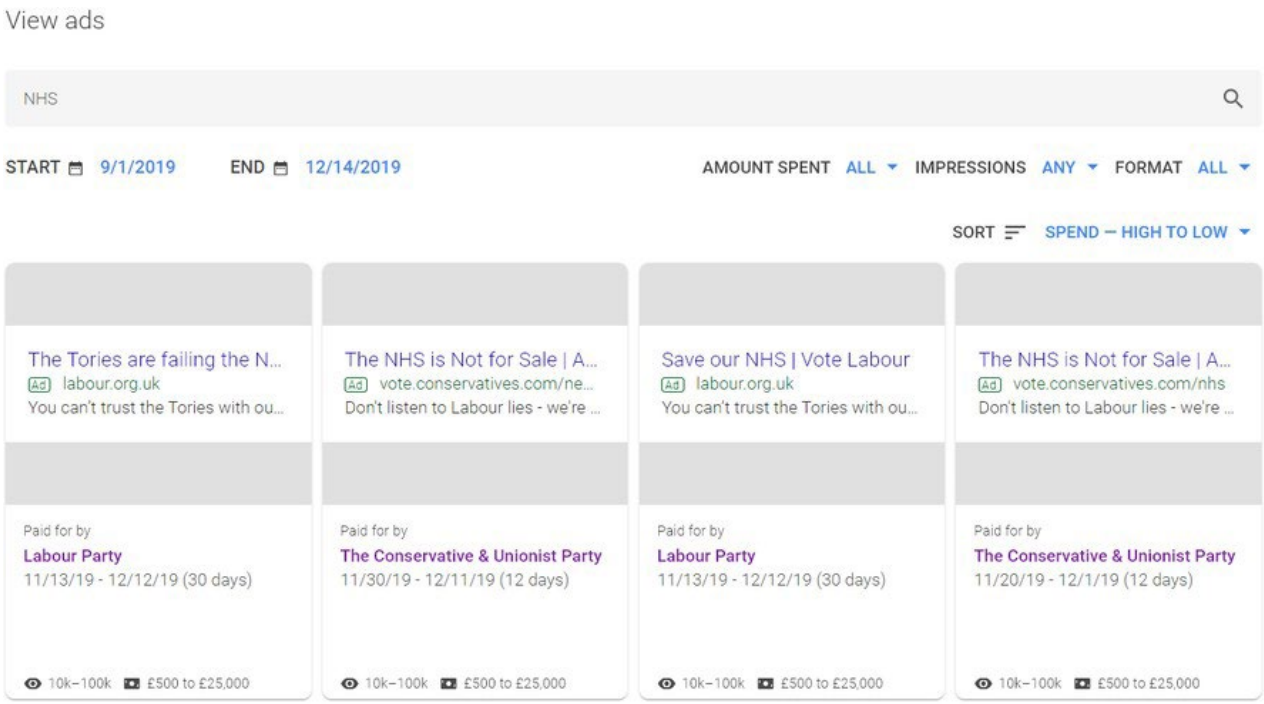


Не е изненадување што најголемите купувања на рекламен простор се случиле непосредно пред и на денот на Општите избори, 12 декември 2019 година. Ќе видите и дека Конзервативната и Унионистичка партија инвестирала по повеќе од 50,000 фунти за две реклами на Јутјуб што се прикажувале само еден ден.

Лабуристичката партија, од друга страна, потрошила повеќе од 50,000 фунти за реклама на страните со резултати од пребарувања на Гугл за промоција на алатка за која велат дека може да им помогне на гласачите да го најдат своето изборно место.

Find your polling station | Plan your journey
Ad labour.org.uk
Use our handy tool to find your polling station Make sure you know where to vote on Thursday 12 December.

Можете да пребарувате и со клучни зборови. Впишете NHS (National Health Service, Национална здравствена служба во Велика Британија) и ќе видите дека во ноември и декември 2019 година и Лабуристичката партија и Конзервативците купиле огласен простор на страниците на Гугл со резултати од пребарување за да ги критикуваат плановите на противниците за НХС.



Со кликнување на името на огласувачот, можете да ги проверите и вкупните суми што ги потрошиле за рекламирање на Гугл од објавувањето на Извештајот за транспарентност. На следната слика се прикажани резултатите за двете водечки политички партии во Велика Британија до јануари 2020 година:

Можете да видите и хронолошки приказ на нивните трошења за реклами. Извештаите од левата страна го прикажува образецот на трошења на Конзервативната и унионистичка партија, а од десна страна се трошењата на Лабуристичката партија.

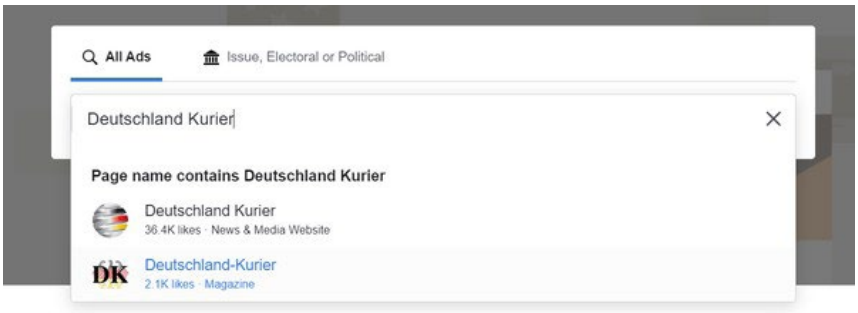
Ако сакате да спроведете натамошна анализа на базата на податоци за рекламирањето, движете се надолу по страницата додека не наидете на зелената секција „download data“ (снимете податоци) што овозможува да ги снимите податоците во „ЦСВ“ (CSV, Comma Separated Values) формат.

Тоа ви овозможува да ги пренесете податоците во програма за сметководствени табели, како што се „Гугл Шитс“ (Google Sheets) или Ексел (Excel) каде можете да вршите дополнително филтрирање и анализа.

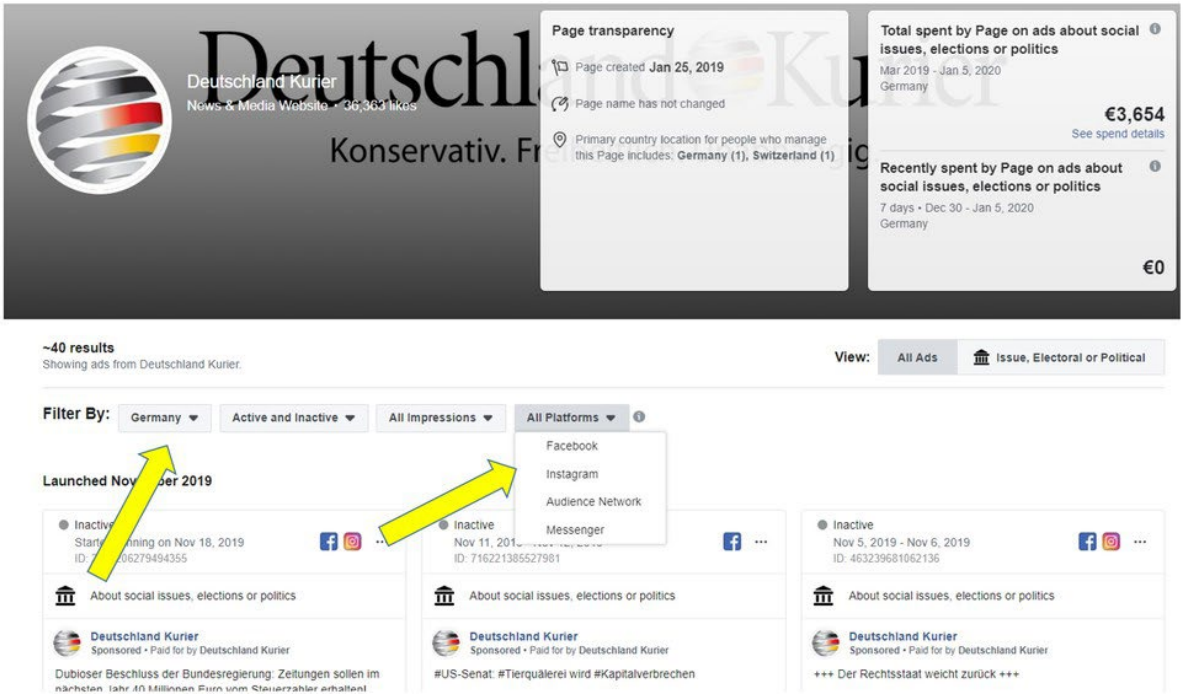
Фејсбук

Библиотеката на реклами на Фејсбук е поделена на два дела: „Сите реклами“ (All Ads) и „Општествено прашање, изборни или политички“ (Issue, Electoral or Political) Ако кликнете на „Сите реклами“ (All Ads) можете да пребарувате специфични огласувачи само по нивното име и не можете да користите и клучни зборови.

На пример, сакам да ги видам рекламите наручани од „Дојчланд курир“ (Deutschland Kurier), публикација што често објавува содржини со поддршка за германската партија од крајната десница АФД (AfD), можам да го внесам името на публикацијата и Фејсбук ќе препорача страници со тој текст:

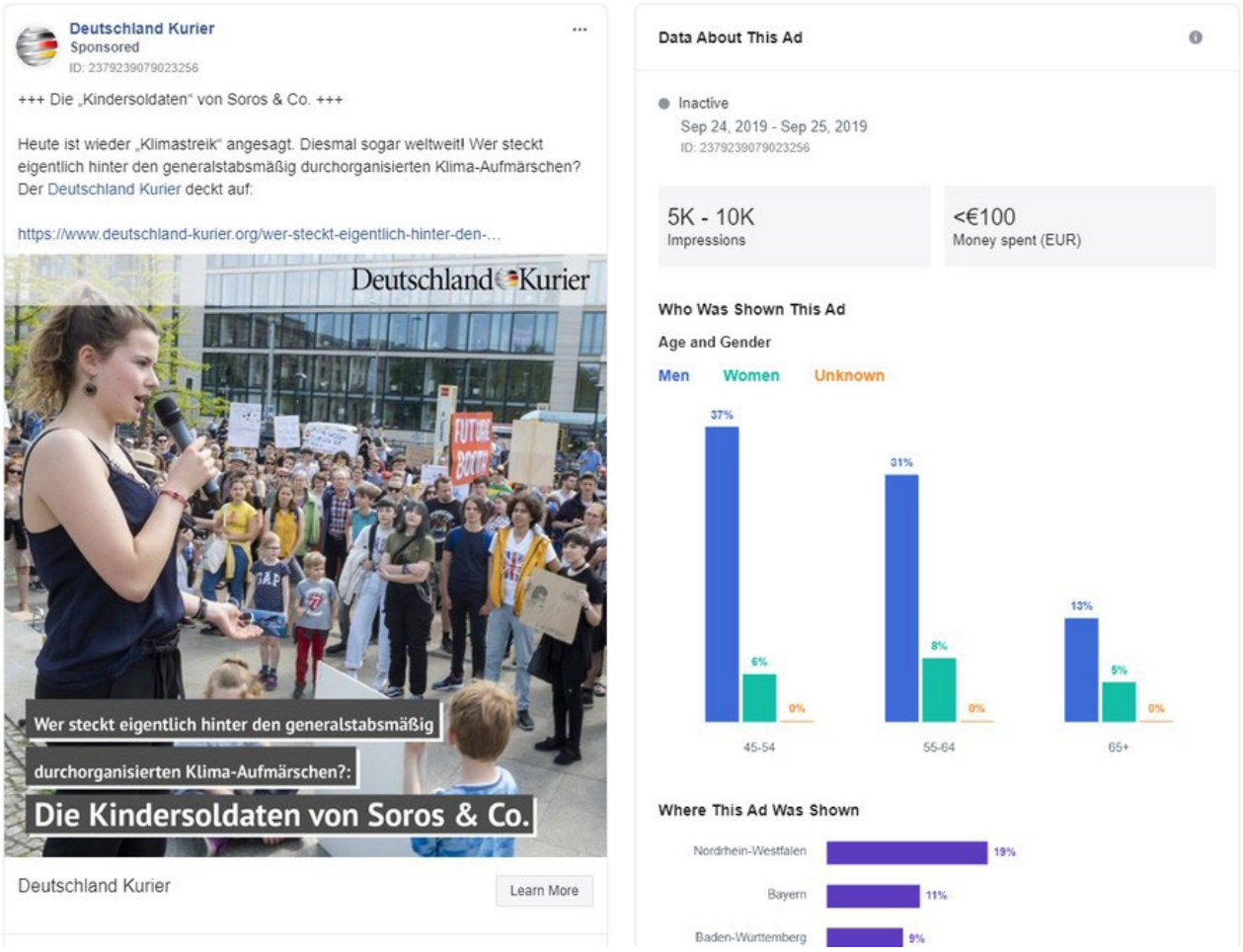


Страницата со резултати покажува дека „Дојчланд Курир“ поставил реклами со вкупна вредност од 3,654 евра во Германија, помеѓу март 2019 и јануари 2020 година.



Кога ќе стигнете на страницата со резултати, задолжително изберете ја соодветната земја во која сакате да пребарувате (или „all“, сите држави), како и дали сакате да ги видите рекламите од Фејсбук, од Инстаграм, од „Месинџер“ (Messenger) или од „Одиенс нетворк“ на Фејсбук (Facebook Audience Network). „Одиенс нетворк“ е мрежа за рекламирање на Фејсбук што поставува реклами на мобилни апликации и интернет страни што не се сопственост на Фејсбук. Во повеќето случаи, најдобар избор е да се пребарува преку сите платформи за да се стекне целосна слика за рекламите што ги нарачала некоја организација.

На секоја индивидуална реклама можете да кликнете на копчето „See ad details“ (Повеќе детали за рекламата) за да прегледате дополнителни информации.



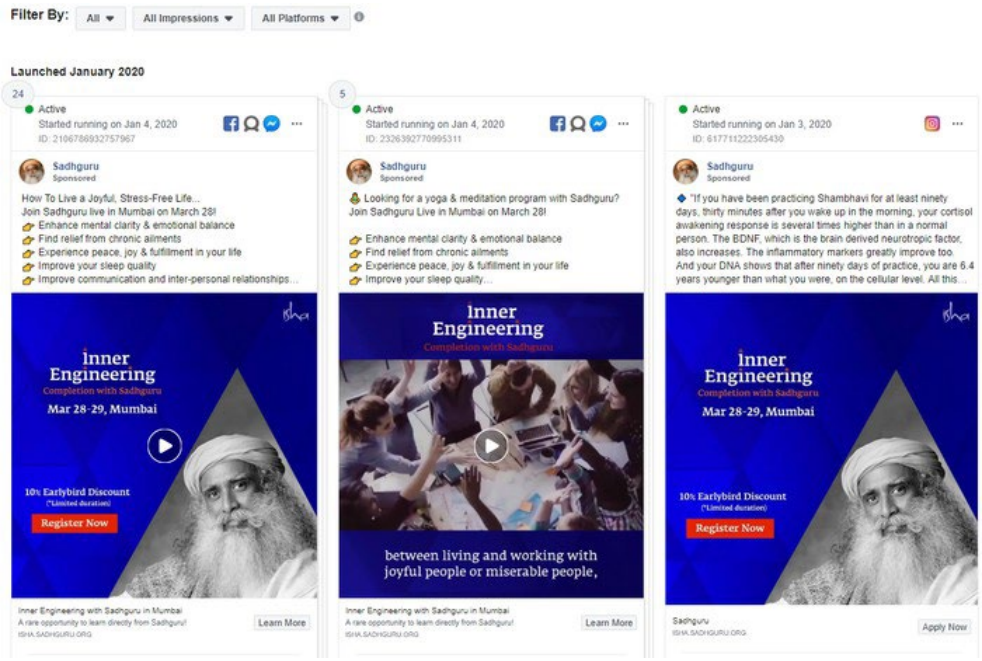
Во овој случај, „Дојчланд Курир“ потрошил повеќе од 100 евра за реклама што ги нарекува луѓето што протестираат за климатските промени „деца-војници на Сорос и компанија“, со помеѓу 5,000 и 10,000 импресии, повеќето прикажувања се на мажи на 45-годишна возраст или постари.

Втората опција за пребарување на библиотеката на реклами е да ја изберете базата на податоци „Општествени прашања, Избори или Политика“, архива на реклами што се занимаваат со општествени прашања, избори или политика. Една голема предност на оваа опција е што можете да пребарувате со клучни зборови ако тоа го сакате, а исто така, Фејсбук ги архивира таквите реклами.

Да погледнеме еден пример.

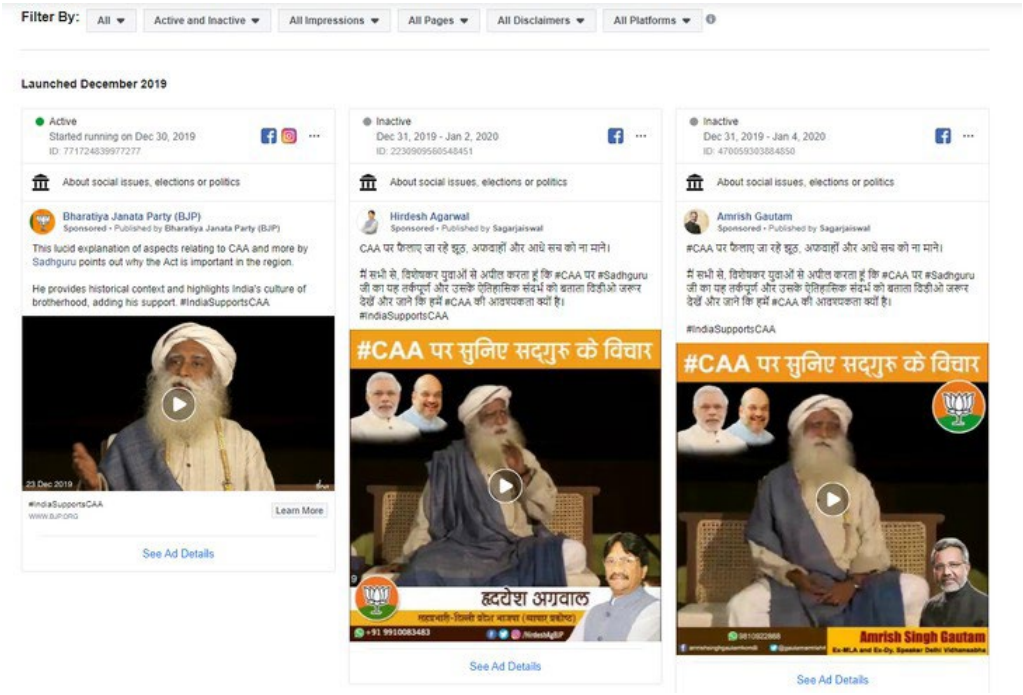
Садгуру (Sadhguru) е името на познат индиски духовен гуру кој вели дека не е поврзан со ниту една политичка партија. Тој има изјавено [дека смета дека му е должност да ја поддржува секоја власт „за таа да го даде најдоброто од себе“](). Ако го внесете неговото име во секцијата „All Ads“ (Сите реклами), Фејсбук ќе понуди како сугестија да ја посетите неговата лична страница на Фејсбук.

Таму е прикажан избор од аполитични реклами објавени од Садгуру и во нив тој ги промовира своите курсеви по јога и медитација.



Да го внесеме сега неговото име во полето за пребарување „Општествени прашања, Избори или Политика“ без да ги прифатиме сугестиите што ги нуди Фејсбук:

Резултатите се драматично различни. Можете да видите колекција од реклами што го спомнуваат Садгуру, објавени од други кориснички сметки.

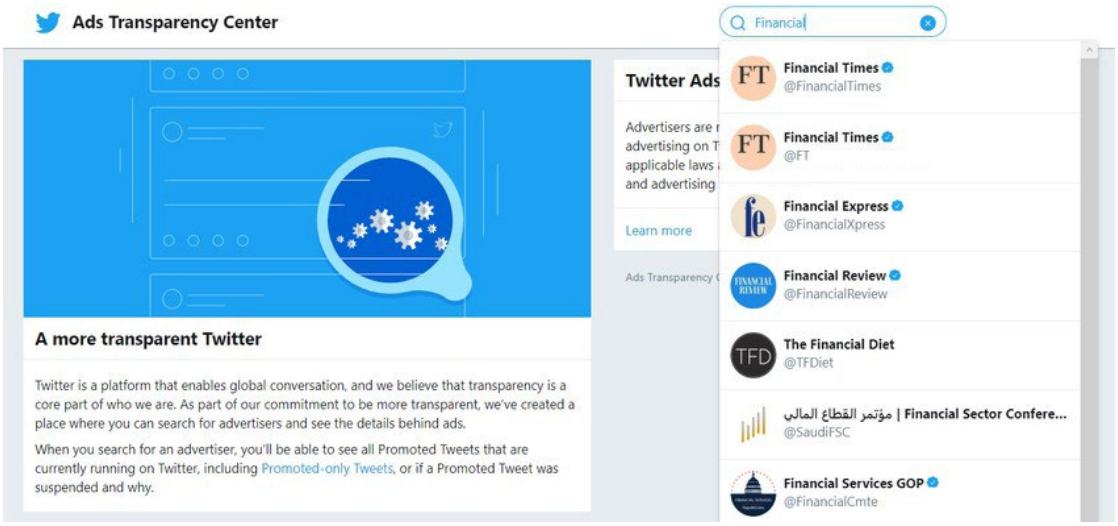


Една реклама на владеачката националистичка партија во Индија „БЈП“ (BJP) прикажува видео во кое Садгуру дава поддршка за контроверзниот законски предлог за Амандманот за државјанство на партијата. Предлогот дозволува нерегистрирани имигранти од некои од соседните земји полесно да добијат индиско државјанство, но не им ја нуди истата можност и на муслиманите. Рекламата укажува на можна врска помеѓу Садгуру и БЈП, тема за која широко се расправа во Индија. Овој пример покажува како може да се користи библиотеката на реклами на Фејсбук за да обезбедите дополнителни клучни информации за вашите истражувања. Можеби ќе посакате да го разгледате и извештајот на библиотеката на реклами на Фејсбук (Facebook Ad library report) во кој се пренесени клучните увиди од политичките реклами во различни држави.

Твитер

Кон крајот на 2019 година, Твитер одлучи да го забрани политичкото рекламирање на својата платформа. Сепак, сè уште е можно да се користи центарот за транспарентност на рекламите на социјалната мрежа за информации за не-политичките реклами од претходните седум дена.

Пронаоѓањето реклами е обемна работа затоа што не постои функција за пребарување со клучни зборови. За да почнете со пребарување, одете на полето во горниот десен агол на екранот и внесете специфично корисничко име или прекар.



Ако има објавено реклами во претходните седум дена, ќе ви бидат прикажани.

Пребарувајќи за „Фајненшел тајмс“ (The Financial Times), можеме да видиме дека весникот платил за да предизвика повеќе интерес за сторијата „Како домородните говорници можат да престанат да ги збунуваат сите останати луѓе“. Твитот е испратен на 3 декември 2019 година, но информациите за рекламата што ги дава Твитер не нудат прецизни детали кој период е покриен од платената промоција.

За да го забрзате пребарувањето, можете да искористите еден мал трик. Откако ќе го спроведете пребарувањето, погледнете ја линијата со УРЛ адресата во прелистувачот:

ads.twitter.com/transparency/FinancialTimes

УРЛ адресите секогаш имаат иста структура, со прекарот даден од Твитер на крајот. Избришете го последниот сегмент од адресата и заменете го со друг прекар:

ads.twitter.com/transparency/Bellingcat

Освежете ја страната и ќе ги видите информациите за рекламите на Белингкет. Ако бараната сметка не објавила реклами во последните седум дена, ќе се појави пораката „This account hasn›t promote any ads in the last seven days“ (Оваа сметка не промовирала никакви реклами во последните седум дена). Бидејќи можете да ги видите само рекламите од претходните седум дена, најдоброто што можете да направите е почесто да проверувате дали саканата корисничка сметка објавувала реклами, и да правите снимки од приказот на екранот секогаш кога ќе забележите нова реклама.

Снепчет

„Библиотеката на политички реклами на Снеп“ (Snap political ads library) дава увид во политичките, рекламите за „општествени прашања“ и застапување. Вторите се дефинирани како „реклами што се однесуваат на прашања или организации што се предмет на расправа на локално, национално или глобално ниво, или се прашања од јавно значење“. Прашања како што се, на пример, имиграцијата, образованието или поседувањето огнено оружје.

Ако ја посетите библиотеката, ќе видите листа на години.

Кликнете на некоја од годините и можете да снимите сметководствена табела со сите достапни информации за рекламите од таа година. Иако на прв поглед не изгледа така, содржината на табелата е мошне возбудлива! Секоја линија претставува една реклама и прикажува кој е нарачателот, колку пари се потрошени на неа, дури и кои карактеристики за микротаргетирање на корисниците биле избрани.

Во горниот пример, огласувачот сакал да таргетира „авантуристи, љубители на култура и уметност, сурфери и луѓе што сакаат да одат на плажа, љубители на третмани за убавина, љубители на книги, универзитетски студенти, гурмани, хипстери и тренд-сетери, консументи на политички вести, љубители на активности во природа, љубители на животни, филантропи, светски патници, женски животни стилови“.

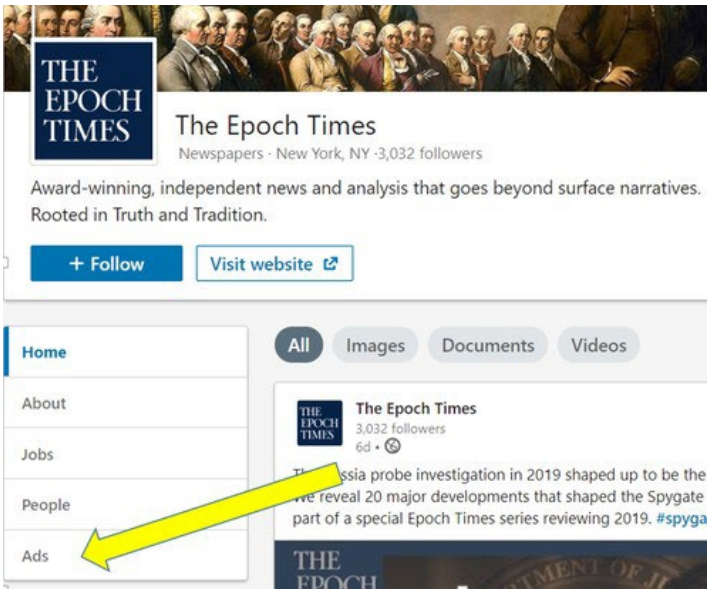
Други платформи не нудат таков вид на приказ на информации за таргетирањето во нивните библиотеки на реклами.

Во табелата можете да пронајдете и УРЛ адреса и да видите како изгледала рекламата.
Во нашиот пример, пронајдов порака што ги охрабруваше луѓето да нарачаат бесплатни знамиња во боите на виножитото како поддршка за претстојниот референдум во Швајцарија во врска со заштитата на ЛГБТ лицата од дискриминација.

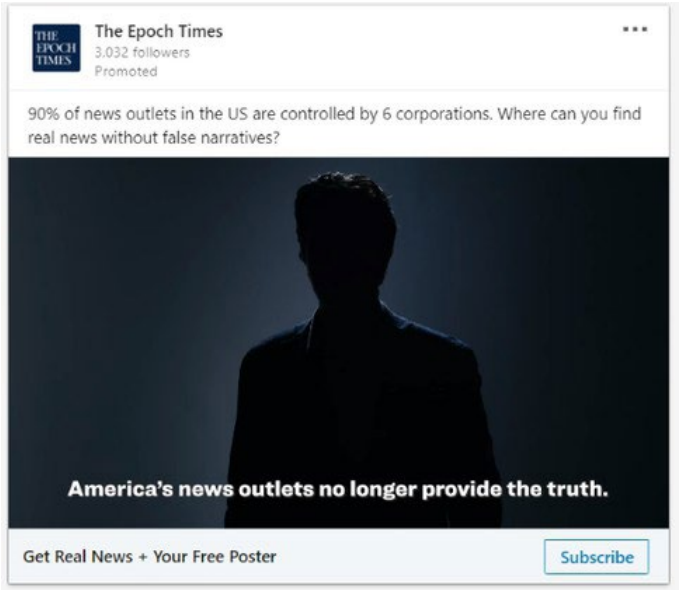
ЛинкдИн

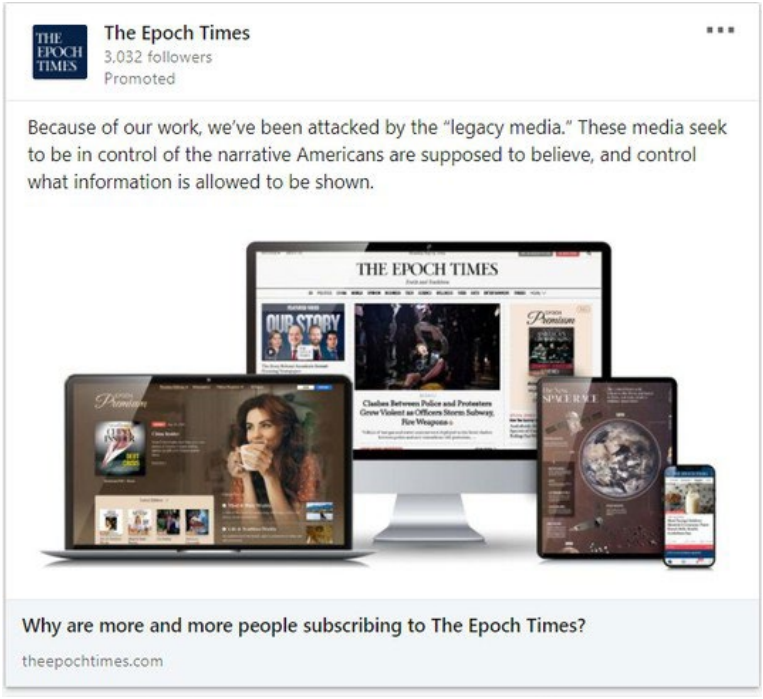
„ЛинкдИн“ не дозволува политички реклами на платформата и нема библиотека на реклами. За среќа, постои друг начин да се добие увид во рекламите што некоја компанија ги поставила на платформата.

Кога ќе ја посетите страницата на некоја компанија на ЛинкдИн, ќе видите јазиче „Ads“ (Реклами) на дното од левата колона.

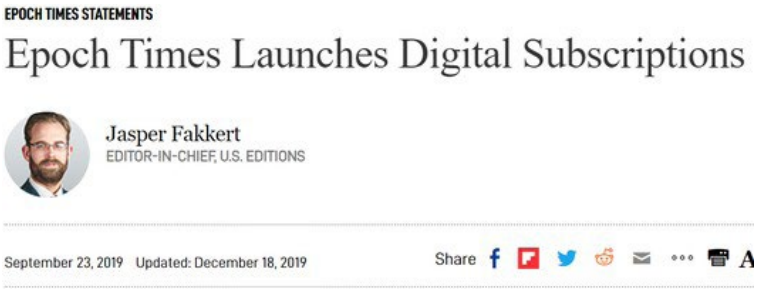


Кликнете на јазичето и ЛинкдИн ќе ви прикаже листа на сите реклами што компанијата ги објавила во претходните шест месеци. Со користење на таа функција, можевме да видиме дека „Ипок Тајмс“ (Epoch Times) сè уште објавуваше реклами на ЛинкдИн откако тоа и беше забрането на Фејсбук. Двете реклами објавени од компанијата тврдеа дека „Американските информативни медиуми веќе не ја кажуваат вистината“ тврдејќи, од друга страна, дека „Ипок тајмс“ е „независен“ и „непристрасен медиум“.





Точните датуми на објавување не се видливи, но можете да кликнете на рекламата (функционира дури и ако таа не е активна на ЛинкдИн) а страницата до која води тој линк понекогаш дава поконкретен датум. Првата реклама на „Ипок тајмс“ водеше до текст со датум 23 септември 2019 година и „Дополнето: 18 декември 2019 година“, што помогна во проценката кога би можела да биде активна.



Кога еднаш ќе ги совладате нивните скриени функционалности, библиотеките за реклами се лесен за користење и моќен додаток на вашиот арсенал за дигитални истраги, и значаен елемент што треба да се провери кога се истражува за некое лице или субјект со присуство на социјалните медиуми.

10. Следење на движењето на актери преку повеќе платформи

Автор: Бен Колинс

Бен Колинс *(Ben Collins) е новинар на ЕнБиСи Њус (NBS News) што ги покрива темите поврзани со дезинформациите, екстремизмот и интернет. Во последниве пет години тој известува за подемот на теориите на заговор, заедниците засновани на омраза, странските кампањи за манипулација и неуспесите на платформите на тоа поле. Претходно работеше во „Дејли Бист" (The Daily Beast) и со неговиот тим ги откри сметките, групите и реалните настани креирани ов руската фарма на тролови „Агенција за истражување на интернет" за време на Изборите во САД во 2016 година.*

На 3 август 2019 година, Патрик Крусиус (Patrick Crusius) влезе во продавницата „Волмарт" (Walmart) во Ел Пасо и смртно застрела 22 лица, мотивиран од идеологијата за белиот национализам. Пред да се упати кон продавницата, тој постави свој манифест на „/pol/" таблата за политички дискусии на 8chan.net, анонимна платформа за испраќање пораки што последниве години прерасна во собиралиште на белите националисти. На /pol/ таблите на „4Чан" (4chan) и „8Чан" (8chan) безмалку и да нема модерација, и до летото 2019 година, 8chan се претвори во собиралиште за содржини и дискусии посветени на насилниот бел национализам.

Делумно поради тода, корисниците на 8chan понекогаш ги известуваат властите и новинарите кога ќе се појави нов, насилен манифест. Тоа го прават преку додавање на коментари под манифестот и преку онлајн дојави до медиумите и органите на прогонот. Кога напаѓачот од Ел Пасо прв пат постави својот манифест - првично беше поставен со погрешен прилог - еден од корисниците одговори „Ало ФБИ". Вистинскиот манифест потоа беше поставен веднаш под коментарот што го повика ФБИ да дејствува.

Тој тип на себе-пријавување може да претставува информација од критично значење за новинарите по настанувањето на такви трагични настани. Во некои случаи, подобронамерни корисници одат на поотворените, мејнстрим, граѓански ориентирани места на интернет како што се Редит или Твитер да ја објават појавата на манифести или сомнителни постови пред масовни стрелби. Тоа е мошне значајно, затоа што лесно може да се случи релевантни постови или коментари на 4chan или 8chan да не бидат забележани.

Анонимните платформи како 4chan или 8chan имаат значајна улога во екосистемите за мисинформации, дезинформации и тролирање на интернет, затоа што на нив луѓето често соработуваат на креирањето и координирањето на кампањи. Редит, друго популарно место каде што се собираат корисници во услови на анонимност, е дом на шаренолик спектар на онлајн-заедници. Некои од таквите под-редити (sub-reddits) се строго модерирани и им помагаат на корисниците да разменуваат приказни за нивните хобија или да расправаат за вестите и настаните; други под-редити се, во основа, места каде сè е дозволено и каде омразата може да се множи без какви било пречки. За новинарите е значајно да знаат како да ги следат и како да известуваат за тие заедници, и да ги познаваат суптилните детали за начинот на кој функционираат.

Следат пет правила што треба да ги почитувате кога настаните од вас бараат користење на 4chan или 8chan (или нејзината понова верзија 8kun) во вашето известување:

1. Не верувајте на ништо што ќе видите на 4chan/8chan.
2. Не верувајте на ништо што ќе видите на 4chan/8chan.
3. Не верувајте на ништо што ќе видите на 4chan/8chan.
4. Некои корисни информации што се однесуваат на (или дури се докази за) кривични дела, кампања за тролирање или дезинформации можат да се пронајдат на 4chan/8chan.
5. Не верувајте на ништо што ќе видите на 4chan/8chan.

Не можам доволно да истакнам колку е важно новинарите да ги следат правилата 1, 2, 3 и 5, дури и ако тоа ги спречува во собирањето на „сочни" детали според правилото број 4. Тие интернет-страни буквално се создавани за тролирање, ширење на двосмислени пораки и лаги за претпоставените непријатели, промовирање на лаги за маргинализираните групи и, повремено, квази-смешни лаги врамени како вистински приказни за тоа како е да се биде тинејџер.

Тоа се гледа од фактот што служат како депозитар за манифести на белите националисти, „инсели" (incel, од involuntary celibate - недоброволен целибат) и други гневни млади стрелци што учествуваат во масовни убиства со огнено оружје.

Да повториме уште еднаш: Ако нешто е поставено на 4chan или 8chan (ќе продолжиме да го нарекуваме така, наспроти формалната промена на името во 8kun), огромни се шансите дека се работи за лага со намера да се предизвика хаос и да се „реметат" новинари. Не влегувајте во некоја дискусија за да побарате повеќе детали. Всушност, не постирајте ништо. Ќе станете цел на луѓе со премногу слободно време.

Потврдување на манифестот

Затоа е од толку голема помош кога членови на тие заедници ќе алармираат за појава на манифести и други содржини што се интересни за известувачите. Коментарот „Ало ФБИ" на 8chan е како дознав за постоењето на манифестот од Ел Паso. Кратко време по извештаите за нападот, го пребарав Твитер со клучните зборови „El Paso 4chan" и „El Paso 8chan". Пребарувањето по формулата „[име на градот] + [8chan или 4chan или incels.co] или други екстремистички интернет страни обезбедува корисен образец што може да се следи и кај други слични настани.

Пребарувањето на Твитер откри дека неколку корисници споделиле снимка од приказот на екранот со постовите на напаѓачот на 8chan, иако повеќето лажно го припишуваа постот на некој што користи 4chan. Значи требаше да го пронајдам тој пост.

Кој е најбрзиот начин да се побара некој пост на 8chan? Гугл. По пукањето, пребарував со фразата „site:8ch.net" а потоа додадов еден дел од реченица од наводниот пост што стрелецот го оставил на 8chan. (Забелешка: 4chan автоматски ги брише постовите од своите сервери по одреден временски период, но постојат автоматски интернет страни за архивирање на 4chan. Најобемниот од нив се нарекува 4plebs.org. Архивираните постови на 4chan можат да се пронајдат со замена на терминот „4chan" во УРЛ адресата со „4plebs", и отстранување на зборот "boards" пред „ x". На пример: boards.4chan.org/pol/13561062.html можете да го пронајдете на адресата 4plebs.org/pol/13561062.html.)

Кај некои напади со огнено оружје, може да се покаже полезно да се обидете да пребарате со фразата „site:4chan.net + ‹manifesto› или ‹fbi›" и да ги искористите опциите на Гугл за да го ограничите периодот на пребарување на претходните 24 часа. Корисниците на „Chan" можеби веќе се обиделе да го пријават стрелецот во одговорите на нивниот пост.

Мојата почетна стратегија не го откри релевантниот пост на 8chan, и тоа ме натера да мислам дека се работи за набрзина склепана измама. Сепак, нешто не беше во ред. На постот на Твитер со снимката од екран имаше кориснички идентификациски број и број на постот. Тие детали ме убедија дека не се работи за едноставен фалсификат, туку за вистински пост. На 8chan, сите постови доаѓаат од корисници со единствен идентификациски број, алгоротамски генериран и наведен до датумот на објавување на постот. Таквиот систем им дозволува на корисниците да имаат статична идентификација за да можат да ги идентификуваат своите постови во дискусијата.

Таквиот систем на кориснички идентификации, попат, е како дознавме кој е „Q“ од теоријата на заговор позната како „QAnon“. Корисниците можат да креираат де факто перманенти кориснички имиња и лозинки со внесување на корисничко име во полето за идентификациски број кога поставуваат пост, следено од знакот „#“, следено од лозинката.

Корисничката идентификација ми помогна да знам дека истото лице што по грешка постави ПДФ документ со името на стрелецот внатре беше истиот корисник што го постави манифестот две минути подоцна. Двата постови ја имаа истата корисничка идентификација, креирана по случаен избор: 58820b.

До корисничката идентификација стои број на постот, донекаде траен артифакт што креира единствена УРЛ адреса за секој пост. Снимката од приказот на екранот на манифестот од Ел Пасо споделен на твитер вклучуваше идентификација на пост “No.13561062.” Како резултат ја имаме УРЛ адресата 8ch.net/pol/res/13561062.html. Таа постапка за добивање на УРЛ адреса можете да ја користите и во 4chan and 8chan.

Во овој случај, постот не постоеше. Мислев дека бил избришан. (Подоцна дознав дека сопственикот на 8chan Џим Воткинс (Jim Watkins) го отстранил откако дознал за неговата содржина.)

Моја последна надеж беше дека некој што го препознал значењето на постот го архивирал некаде. За среќа, еден корисник на 8chan што брзо размислувал го зачувал постот на архивската интернет страна archive.is. Внесувањето на УРЛ адресата во полето „I want to search the archive for saved snapshots“ (Сакам да ја пребарам архивата за зачувани слики) на archive.is откри дека постот со манифестот е автентичен и можев да го прегледам.

Наидов на нов проблем: Кога бил прв пат поставен на 8chan? Ми требаше точна ознака за времето за да потврдам дека манифестот бил поставен пред напаѓачот од Ел Пасо да тргне во поход.

4chan и 8chan ги локализираат ознаките за времето, што ја комплицира задачата на одредување на реалното време од интернет страните за архивирање. За среќа, постои потврден начин да се заобиколи тој проблем. Со десен клик на ознаката за време и избор на „inspect element” ќе ви се прикаже изворниот код на интернет страната, и на неа е истакната секцијата што почнува со фразата „<time unixtime=‘[number]“.

Копирајте го и внесете го тој број во некој конвертор за временски ознаки „Ипок/Уникс“ (Epoch/Unix), како што е unixtimestapm.com, и ќе добиете до секунда точна временска ознака на постот по Гринич (UTC). Конверзијата од UTC во временската зона во која се наоѓа Ел Пасо открива дека манифестот е поставен во 10.15 часот наутро Централна временска зона (Central Time) - неколку минути пред да почне нападот.

Постапката ми помогна да потврдам дека манифестот поставен на „8chan manifesto“ беше легитимен доказ во случајот на расистички домашен тероризам.

Следење на движењето на актери преку повеќе платформи

Во 2017 година, Лејн Дејвис (Lane Davis), поранешен „истражувач на Гејмергејт“ (Gamergate, кампања за вознемирување жени во индустријата на видео игри) (читај, професионален демнач на интернет) што работеше за посрамениот гуру на алтернативната десница Мило Јанопулос (Milo Yiannopoulos), го уби својот татко во неговиот дом.

Дејвис влегол во кавга со родителите, а повикот до бројот за итни случаи 911 открива дека „блуел“ екстремистички жаргон што крајната десница го користи на интернет пред нападот. Ги нарекол родителите „левичарски педофили“ пред татко му да повика полиција да му помогне да го исфрли Дејвис од нивниот дом, каде што син им сè уште живеел.

На интернет Дејвис беше познат како „Seattle4Truth“ (Сиетл за вистината), а во неговите видеа на JyTjуб често спомнувал фиктивни тајни педофилски кругови за кои верувал дека се движечката сила на либерализмот. Едно од видеата на JyTjуб објавени под неговото име носеше наслов „Длабоките врски на прогресивната идеологија со педофилијата“.

За известувачите што го истражуваат екстремизмот на интернет ситуација кога сторителот користи статично корисничко име на сите платформи е сценарио од сништата, а токму тоа беше случај со Дејвис. Тој се идентификуваше како „Seattle4Truth“ на JyTjуб но и на Редит, каде неговите постови откриваат ум уште повеќе оптоварен со заговори.

Како го откривме тоа? Едноставно го внесовме корисничкото име seattle4truth во линијата на УРЛ адресата за кориснички имиња на Редит: reddit.com/u/[username]. Еднаш влезени, можете да ги подредувате постовите од најнов кон најстар, по популарност, по „контроверзност“ (ги подредува постовите според комбинација од бројот на гласовите за поддршка и спротивставување што ги добиле).

Еден брз начин да проверите некое корисничко име е преку „Namechk“, алатка што пребарува кориснички имиња во скоро 100 интернет сервиси. Како што посочувам подолу, тоа не значи дека исто лице управува со сите сметки, но е ефикасен начин да се види каде сè се користи корисничкото име за да можете да го насочите пребарувањето. Исто така, за кое било корисничко име за кое сте заинтересирани можете да извршите пребарување на Гугл.

Треба да сте свесни за видот на заедници на интернет што функционираат како супер-ниши на кои вашата цел би можела да биде активна. Вилијам Едвард Ечисон (William Edward Atchison), кој изврши напад со огнено оружје во училиште во Њу Мексико во 2017 година, беше идентификуван од корисниците на „КивиФармс“ (KiwiFarms), интернет страна посветена првенствено на малтретирање на транс-родови лица, како корисникот @satanicdruggie. Корисниците велеа дека бил активен на „Енциклопедија Драматика“ (Encyclopedia Dramatica), интернет страна за „мимови“ на која се поминува и на која понекогаш може да се пронајде екстремистичка реторика.

Ачисон не само што беше активен на Енциклопедија Драматика, туку имаше позиција системски оператор (SysOp), значи администратор и корисник со посебни овластувања. (Корисници на интернет страната што развиле односи so Ачисон во реалноста, главно преку Скајп (Skype), ни потврдија дека сметките се негови. Ачисон доброволно ги насочувал корисниците кон своите други сметки, во случај да биде „баниран“.) Пребарувањето на Гугл со неговото корисничко име во линијата „site:encyclopediadramatica.rs + [username]” откри дека покрај „Сатаник Драги“ (Satanic Druggie - сатанистички наркоман), користел и други имиња како „Иден напаѓач на училиште“ (Future School Shooter) и „Адам Ланца“ (Adam Lanza), името на напаѓачот од Сенди Хук (Sandy Hook).

Историјата на неговите постови на интернет укажува на опсесија со напади на училишта што дури ни полицијата не ја откри по нападот.

Повторно, значајно е да се нагласи дека присуството на едно корисничко име на повеќе платформи не гарантира дека сметките се креирани од едно лице. Во еден познат пример, ноторните агенти за крајно-десничарски дезинформации Јан Мајлс Чеонг (Ian Miles Cheong), Мајк Цернович (Mike Cernovich), „ИнфоВорс“ (InfoWars) и „ГејтвејПандит“ (GatewayPundit) сите тврдеа дека човекот што уби две и рани 10 лица на турнирот во видео игри во Џексонвил (Jacksonville) бил анти-Трамповец.

Причината за таквото тврдење? Напаѓачот, Дејвид Кац (David Katz) го користел корисничкото име „Ravens2012Champs“ на онлајн турнири за видео игри, а еден анти-Трамп корисник на Редит имал слично корисничко име: „RavenChamps.“

Известувањето беше толку брзо и во еден здив колку што беше неточно. Насловот на „ИнфоВорс“ гласеше „Полудениот напаѓач од Џексонвил ги критикувал ’Трамптардите’ на Редит“ (Jacksonville Madden Shooter Criticized ‘Trumptards’ on Reddit), а приказната тврдеше дека тој ги „мразел поддржувачите на Трамп“.

RavenChamps, како што се покажа, е сосема друго лице, фабрички работник од Минесота по име Павел.

„Знаете, јас сум жив?“ напиша тој на Редит неколку часови по нападот. (Вистинскиот напаѓач се самоуби по масакрот.)

Потребно е многу повеќе од корисничко име, но тоа може да биде клучната почетна точка за натамошното известување, преку контакти со органите за безбедност, копање по јавните архиви и телефонски разговори.

Следење на кампањите скоро во реално време

Кампањите за дезинформирање и медиумски манипулации често се шират преку Редит и 4chan, и некои од нив можат да се следат и во реално време.

На пример, 4chan со години се занимава и со местење на онлајн-анкети како поддршка за преферираните кандидати на избори. Во 2016 година, корисници на 4chan повторено поставуваа линкови до национални и хипер-локални информативни интернет страни што спроведуваат анкети пред дебатите на кои учествуваше Доналд Трамп, претпочитаниот кандидат на корисниците.

Поставувањето на параметрите за пребарување на Гугл да ги филтрираат постовите од „последниов час“ (last hour), и пребарување на фразата „site:4chan.org ‘polls’“ ќе ви обезбеди добар увид во анкетите што корисниците на 4chan се обидуваат да ги манипулираат во реално време.

Таа пракса продолжи длабоко во следниот изборен циклус. Анкетите на 4chan ја поддржуваа Талси Габард (Tulsi Gabbard), која ја нарекуваа „Мама“ (Mommy), во анкетите на „Драџ рипорт“ (The Drudge Report) и NJ.com. Преку едноставно пребарување на Гугл на претходно наведениот начин, секој може да види како резултатите од анкетата се менуваа во реално време откако еден корисник на 4chan (channer) им кажа на корисниците „GIVE HER YOUR POWER“ (Дајте и ја својата сила).

Дури и полесно е да се набљудуваат активни операции за тролирање на сајтовите како што е „r/The_Donald“ заедницата на Редит, поради корисната алатка за „подигање“ на Редит.

Користењето на линијата „reddit.com/r/[subreddit-name]/rising“ ги прикажува резултатите што растат со необична брзина на под-редитот секој час.

Можете да ги разгледате и постовите што имаат неочекувано добри резултати на цел Редит (reddit.com/r/all/rising). Таа постапка ги индексира сите постови во најголемиот број заедници на Редит. Пребарувањето не ги опфаќа под-редитите ставени во карантин, „токсични“ заедници со историја на жестоко навредливи содржини што таргетираат други заедници со кампањи за тролирање. Под-редитите ставени во карантин не се индексираат ниту на Гугл, но линијата за пребарување „reddit.com/r/[subreddit-name]/rising“ ќе функционира и за нив. Карантините функционираат одлично во ограничувањето на досегот на кампањите за тролирање надвор од централизирани публики, но потешко се следи како злонамерните актери се организирани во даденият момент.

Генерално, добра идеја е да се држат на око деловите од заедниците познати по кампањи за тролирање што се во пораст, на пример „r/the_donald“, за време на големи политички настани, трагични настани и избори.

Во реалноста, понекогаш активностите на платформите да ги потиснат злонамерните актери може да им отежни на новинарите во вршењето на значајни активности. Алатките можат да помогнат, но најголем дел од работата се врши рачно и бара приоди кон верификацијата што алгоритмите и компјутерите не можат да ги репродуцираат.

На крајот на краиштата, компјутерот не може да го замени човекот за тој вид на работа. Сè зависи од нас.

11. Анализа на мрежи и атрибуција

Автор: Бен Ниммо

Бен Нимо *(Ben Nimmo) е директор за истражувања во „Графика" (Graphika) и не-резидентен виш соработник на Истражувачката лабораторија за дигитална форензика на Атлантскиот Совет (Atlantic Council›s Digital Forensic Research Lab). Неговата потесна специјализација е на полето на големите операции за информирање и влијание што истовремено се одвиваат на повеќе платформи. Слободното време го минува под вода, во нуркање, каде што не е достапен по телефон.*

За секој истражувач што работи на сомнителна информативна операција, клучни прашања се колкав е обемот на операцијата и колку далеку е раширена. Тоа не е исто со мерењето на влијанието и ефектот на некоја операција, што исто така е значајно: Се работи за пронаоѓање на корисничките сметки и интернет страни со кои управува самата операција.

За истражувачот целта е да пронајде што повеќе за операцијата пред да известува за неа, затоа што еднаш кога сме известиле за неа, треба да очекуваме е дека операторите ќе се скријат - потенцијално со бришење или напуштање на други локации.

Првата алка во синџирот

Во секоја истрага, најтешко е да се најде првата индиција или доказ. Често истрагата ќе почне со дојава од загрижен корисник или (што е поретко) од социјална медиумска платформа. Работата на Истражувачката лабораторија за дигитална форензика за разоткривање на сомнителната операција на руското разузнавање „Секундарна инфекција" (Secondary Infektion) почна со дојава од Фејсбук, каде беа откриле 21 сомнителни сметки на платформата. Работата кулминираше шест месеци подоцна кога „Графика", „Ројтерс" и „Редит" го разоткрија обидот, во склоп на истата операција, за мешање во изборите во Велика Британија. Една истрага за дезинформации насочена против воените ветерани во САД почна со откритие од вработен во здружението „Виетнамски ветерани на Америка" (Vietnam Veterans of America) дека една страница на Фејсбук со двојно повеќе следбеници од нивното реално присуство на платформата лажно се претставува во име на групата.

Не постои едно единствено правило за идентификување на првата алка во синџирот со користење на сопствените ресурси. Најефективна стратегија е да барате што е тоа што отскокнува од околината. Можеби се работи за сметка на Твитер што навидум потекнува од државата Тенеси но е регистрирана на руски број на мобилен телефон; можеби е страница на Фејсбук што за себе тврди дека е од Нигер, но е управувана од Сенегал и од Португалија. Можеби е сметка на JyTjуб со милион прегледи што објавила огромни количества на про-кинески содржини во 2019 година, а безмалку сите прегледи доаѓаат преку епизоди од британски ситуациони комедии поставени во 2016 година.

Можеби е анонимна интернет страна фокусирана на американската надворешна политика, но е регистрирана од Одделот за финансии на Далекуисточниот воен округ на Руската Федерација. Можеби се работи за наводно интервју со „агент на МИ6" напревено на крут, безмалку шекспиријански англиски јазик. Може дури да биде и сметка на Твитер што ги прошарува поканите да се посети една порнографска интернет страна со нецелосни цитати од „Разум и чувства" од Џејн Остин.

Кај сите такви сигнали, трикот е да си обезбедите доволно време добро да размислите за нив. Истражувачите и новинарите толку често се под притисок на времето што лесно ги отфрлаат сигналите, мислејќи „чудно ми чудо" и продолжуваат понатаму. Понекогаш, ако нешто е чудно, тоа е чудно со причина. Земањето малку време да се праша „Тоа е чудно: Зошто е чудно?" може да биде првиот чекор во откривањето на нова операција.

Извори, **однесување**, **содржини**

Кога почетниот извор - на пример, корисничка сметка или интернет страна - е идентификувано, следниот предизвик е да се открие каде води. Клучни се три прашања, моделирани според „Абецеда на дезинформациите“ (Disinformation ABC) на Камиј Франсоа (Camille François):

- Какви информации се достапни за почетниот извор?
- Како се однесуваше изворот?
- Каква содржина поставил?

Првиот чекор е да се соберат што повеќе информации за иницијалниот извор. Ако се работи за интернет страна, кој и кога ја регистрирал? Дали има некакви знаци за препознавање, како што е код од Гугл Аналитикс или број од АдСенс, дали во регистрацијата има оставено е-меил адреса или телефонски број? Овие прашања можат да се проверат со реферирање на историските архиви „WhoIs“ што ги нудат сервиси како што се lookup.icann.com, domaintools.com, domainbigdata.com или сервисот со обеспокојувачко име spyonweb.com.

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

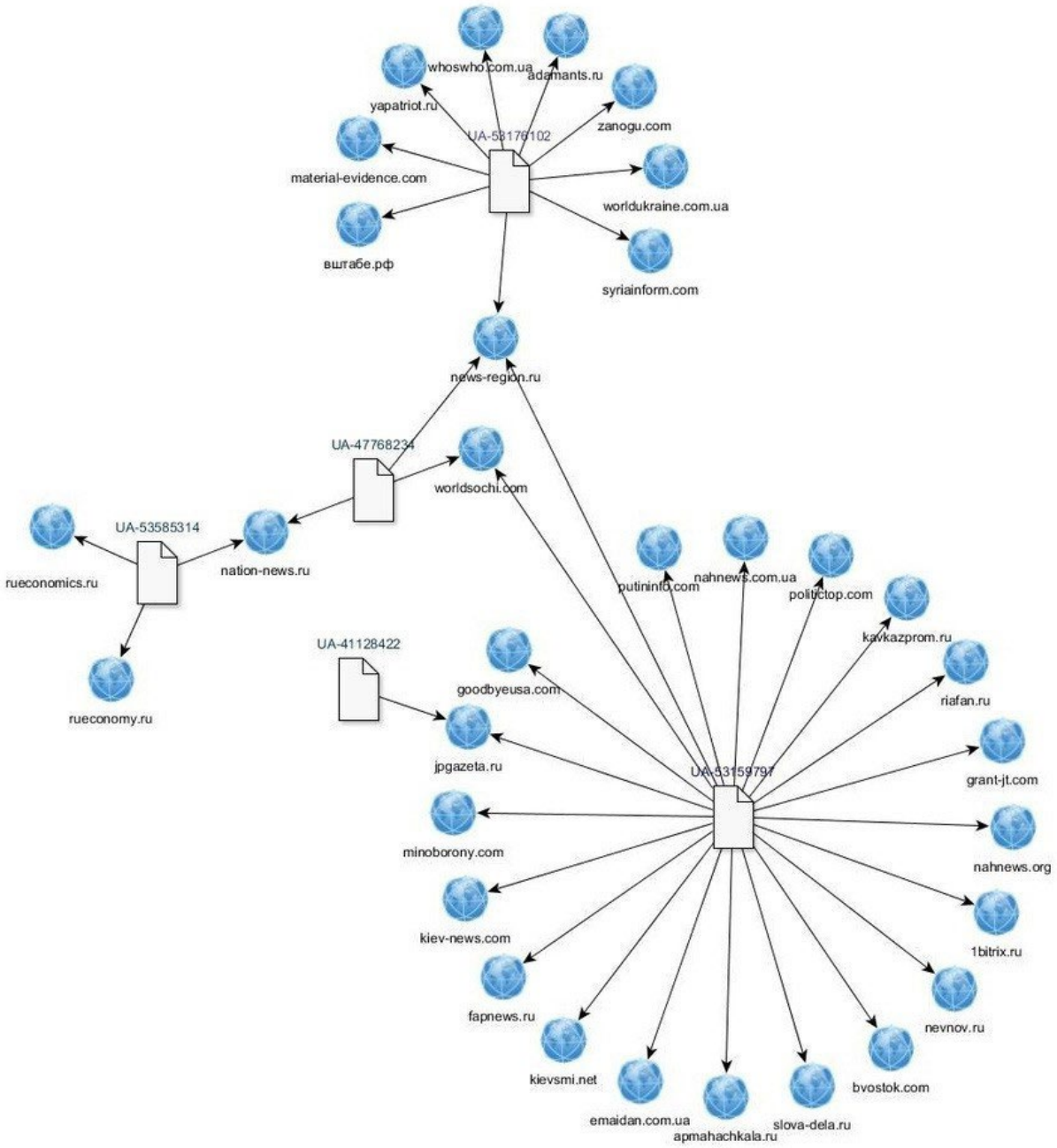
Registrant:

Name: Finance Department of the Far Eastern Military district

Податоците за регистрацијата на интернет страната NBeneGroup.com, која тврдеше дека е „Младинска аналитичка група“, покажуваат дека регистрацијата припаѓа на Финансиското оддел на Далекуисточниот воен округ на Руската Федерација, според lookup.icann.org.

Информациите за интернет страната можат да се искористат за барање на други извори.
И domaintools.com и spyonweb.com им овозможуваат на корисниците да пребаруваат со индикатори како што се АјПи адреси или Гугл Аналитикс кодови, што би можело да води кон поврзани интернет страни - иако повештите информативни операции денес типочно при регистрирањето се кријат зад комерцијални субјекти или услуги за заштите на приватноста, што ја отежнува постапката.

Една од [првите анализи](#) на британскиот истражувач Лоренс Александер идентификуваше 19 интернет страни раководени од руската „Агенција за истражување на интернет“ со следење на нивните броеви на Гугл Аналитикс. Во август 2018 година, фирмата за обезбедување „ФајрАј“ (FireEye) откри обемна иранска операција за стекнување влијание со користење на податоците за регистрацијата, вклучувајќи и адреси за електронска пошта, за да ги поврзи навидум неповрзаните интернет страни.



Мрежа од сродни интернет страни, поврзани преку кодовите од Гугл Аналитикс (осумцифрени броеви со префикс *UA),* идентификувана од британскиот истражувач Лоренс Александер.

Ако почетниот извор е сметка на некој социјален медиум, се применуваат упатствата од претходните две поглавја за ботовите и за неавтентичните активности, како и за истражување на сметките на социјалните мрежи. Кога е создаден? Дали името на екранот се совпаѓа со прекарот? (Ако прекарот е @moniquegrieze а името на екранот е „Simmons Abigayle“, можно е сметката да била киднапирана или да е дел од масовен напор за креирање на кориснички сметки.)

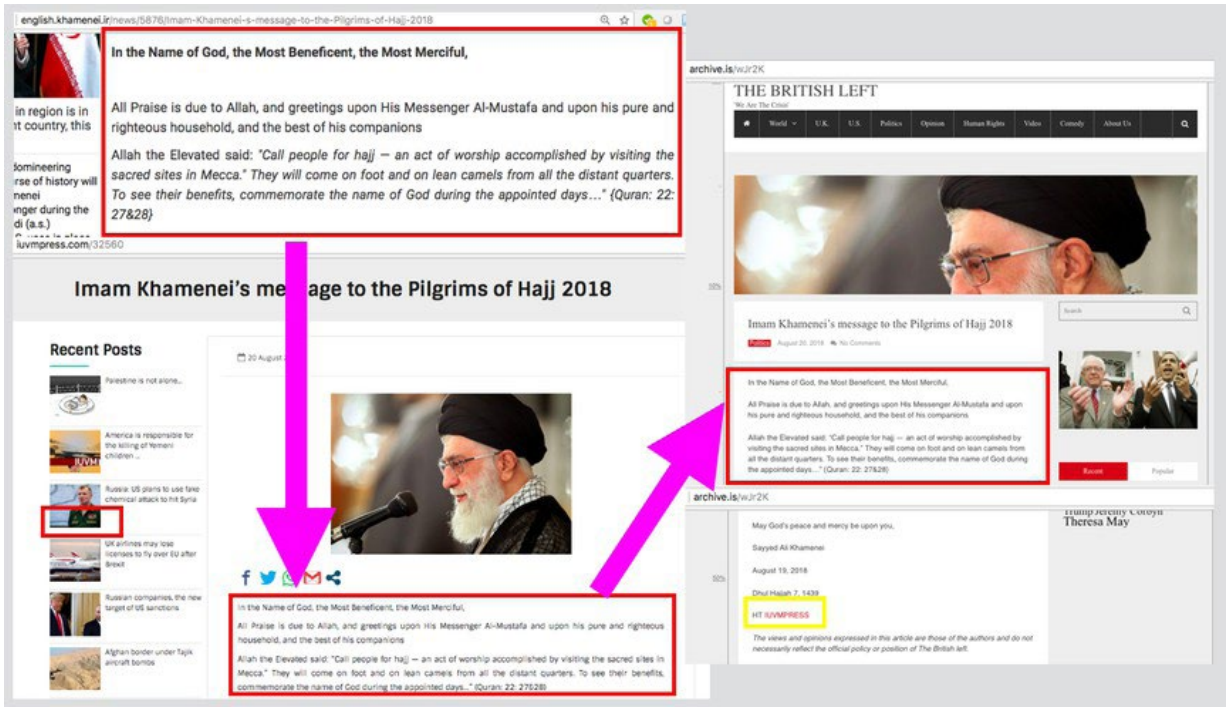
Три сметки на Твитер вмешани во [голема операција со ботови](#)во август *2017* година. Споредете ги имињата на екранот со прекарите, што укажува дека најверојатно се работи за киднапирани сметки, преименувани или пренаменети од гоничот на ботовите.

Дали нуди биографски податоци што можат да се верификуваат, или линкови до други извори на таа или на друга платформа? Ако се работи за страница или група на Фејсбук, кој управува со неа, каде се лоцирани тие што управуваат со неа? Кого следи и кој ја следи? Поставките „Page transparency“ (Транспарентност на страница) и „group members“ (членови на групата) често даваат корисни насоки, исто како и функции на профилите на Твитер како што се датумот на пристапување и вкупниот број на твитови и допаѓања. (На Фејсбук и на Инстаграм не може да се види датумот кога е креирана сметката, но датумот на поставување на првата профилна фотографија претставува разумна замена за тие податоци.)

Транспарентност на интернет страната и на страницата на фејсбук за наводната страна за проверка на факти „C'est *faux — Les fake news du Mali" (Лага е* — лажни вести од Мали), покажува дека иако страната тврди дека со неа раководи група студенти од Мали, всушност е администрирана од Португалија и Сенегал. Слика од *DFRLab*.

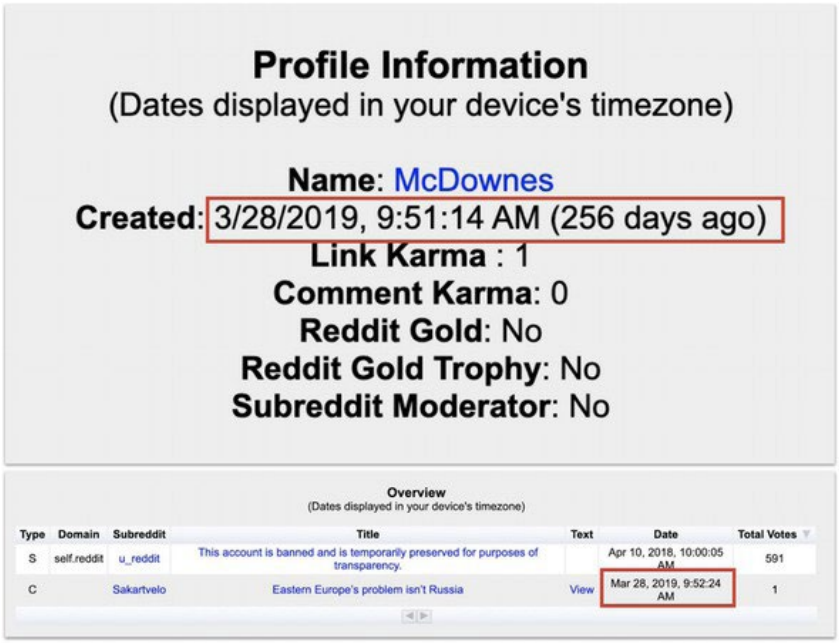
По снимањето на податоците за изворот, следниот чекор е да се карактеризира неговото однесување. Тест-прашањето е, „Кои бихејвиорални одлики се најтипични за овој извор и можат да се искористат за идентификација на други извори вклучени во истата операција?“

Прашањето е опсежно и може да има многу одговори, од кои некои можат да се појават дури во подоцнежните фази на истрагата. Може да вклучува, на пример, канали на JyTjyб со западни имиња и профилни слики кои објавуваат политички видеа на кинески јазик, прошарани со големи количества на кратки „ТикТок“ (TikTok) видеа. Може да вклучува мрежи од сметки на Фејсбук или на Твитер што секогаш споделуваат линкови до иста интернет страна или иста колекција од интернет страни. Може да вклучува сметки што користат исти фрази, или мошне слични варијации на исти фрази во биографските белешки. Може да вклучува „новинарски“ персони без биографски податоци што можат да се верификуваат, или да понуди податоци што можат да бидат препознаени како лажни. Може да вклучува интернет страни што плагираат најголем дел од објавените содржини од други страни, и повремено вметнуваат пристрасни, полемични или заведувачки статии. Може да вклучува многу такви фактори: Предизвикот пред истражувачот е да идентифкува комбинација од особини што ќе му дозволи да каже „Овој извор е дел од оваа операција“.



Обрасци на однесување: Статија изворно поставена на интернет страната на иранскиот ајатолах Хамнеи (Ayatollah Khamenei) и подоцна репродуцирана без наведување на изворот од IUVMpress.com и britishleft.com, две интернет страни што се дел од иранска пропагандна мрежа. Слика од *DFRLab*.

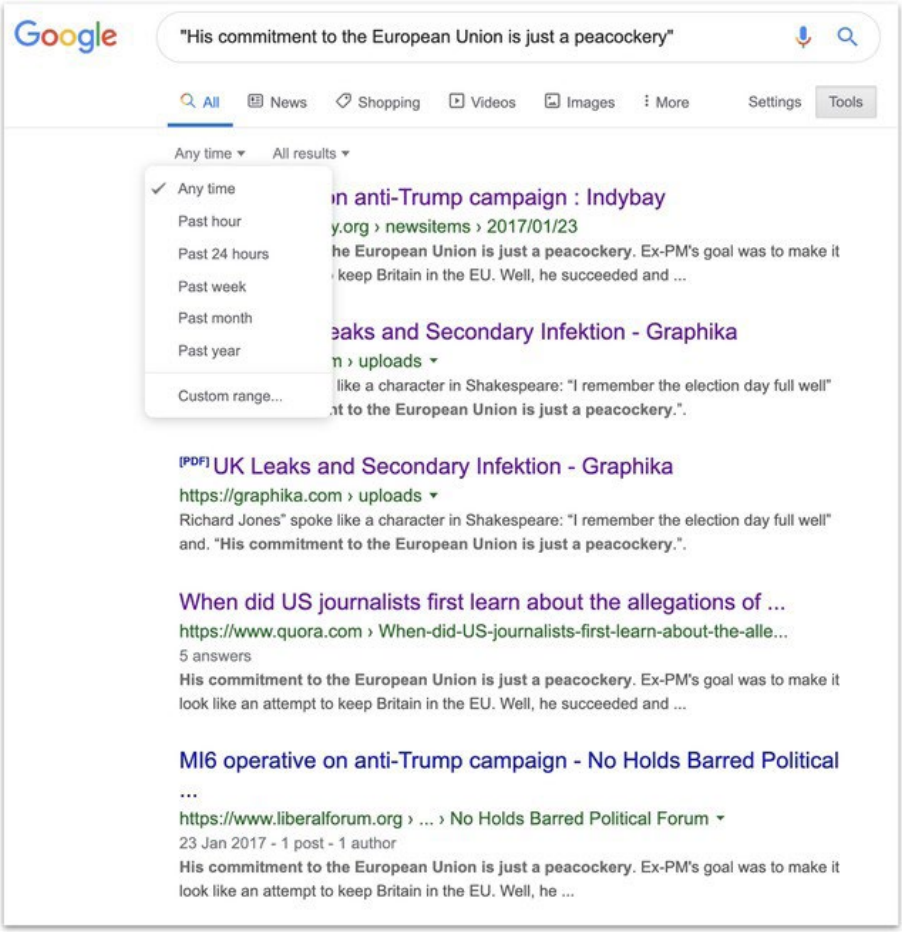
Понекогаш недостигот од идентификувачки особини може самиот да биде идентификувачка особина. Тоа беше случај со кампањата „Секундарна инфекција“ (Secondary Infektion) водена од Русија. Кампањата користеше стотици кориснички сметки на различни блогерски платформи, сите со минимални биографски податоци за авторите, со поставена една статија на денот на отворањето и потоа напуштени за никогаш повеќе да не бидат користени. Овој образец на однесување беше толку конзистентен во толку многу сметки што стана јасно за време на истрагата дека тоа е „потписот“ на операцијата. Кога анонимни сметки почнаа да објавуваат „протечени“ документи за трговијата помеѓу САД и ВБ непосредно пред британските општи избори во декември 2019 година, „Графика“ и „Ројтерс“ покажаа дека тие целосно одговараат на тој „потпис“. Редит ги потврди наодите на анализата.



Профилот на Редит за сметката по име „McDownes“, припишана од Редит на руската операција „Секундарна инфекција“. Сметката е креирана на 28 март 2019 година, поставила само една статија една минута по креирањето и оттогаш потонала во молк. Сликата е од *Graphika,* податоците од *redective.com.*

Индикативни знаци во содржините можат да помогнат во идентификацијата на изворите што се дел од иста мрежа. Ако познат извор сподели фотографија или „мим“, ќе биде корисно да се направи реверзибилно пребарување на сликата за да видите на кое друго место била искористена. „РевАј“ (RevEye) додатокот за прелистувачи е особено корисна алатка затоа што им овозможува на истражувачите да спроведуваат реверзибилно пребарување преку Гугл, Јандекс, ТинАј, Баиду (Baidu) и Бинг (Bing). Секогаш се исплати користењето на повеќе пребарувачи, затоа што тие често даваат различни резултати.

Ако изворот сподели некој текст, добро е да се побара дали тој текст се појавил и на друго место. Кај подолгите текстови пожелно е да изберете една или две реченици од третиот или од четвртиот параграф, или подолу во текстот, затоа што операциите за залажување знаат да ги преработат насловот и воведот од статиите што ги копирале, додека можноста дека го преработиле главниот текст е помалку веројатна. Внесувањето на избранион исечок во наводници во пребарувачот на Гугл ќе ви ги прикаже сите совпаѓања. Менито „tools“ (алатки) може да ги подреди резултатите по датум на објавување.



Резултатите од пребарување на Гугл на фраза објавена од сомнителна руска операција со приказ на функцијата на Гугл за ограничување на пребарувањето по датум.

Изворите што поставуваат текстови со грешки се особено корисни затоа што грешките по природа се поневообичаени од правилно напишаните зборови. На пример, една статија објавена во рамките на претпоставена операција на руското разузнавање го пишува името на британскиот град Солзбери, каде беше отруен поранешниот руски агент Сергеј Скрипал (Sergei Skripal), „Solsbury“ наместо „Salisbury“ како што правилно се пишува на англиски. Тоа придонесува за многу подобро таргетирано пребарување на Гугл со многу помалку резултати од пребарувањето со термините „Skripal“ и „Salisbury“. Тоа значи дека добивате многу поголем удел на значајни наоди во резултатите.

Кога барате индиции во содржината, особено е значајно да ги погледнете и другите индикатори, како што се обрасците на однесување, за да потврдите дали некој извор е дел од поголема операција. Постојат многу легитимни причини зошто несвесните корисници споделуваат содржини што потекнуваат од информативни операции. Тоа значи дека споделувањето на содржини од некоја операција е слаба индиција. На пример, многу корисници споделувале „мимови“ од руската Агенција за истражување на интернет затоа што тие имаат вистински вирални особини. Само споделувањето на содржини не е доволно да се означи некој како средство на поголема операција.

Собирање докази

Информативните операции и операциите за влијание се сложени и се движат со огромна брзина. Едно од најфрустрирачките искуства за истражувач на отворени извори е да види како збирка на извори се исклучува од интернет среде истражувањето. Оттаму, клучно правило во анализата е снимај ги и архивирај ги веднаш штом ќе ги пронајдеш, затоа што можеби нема да имаш втора шанса.

Различни истражувачи имаат различни преференци околу зачувувањето на изворите што ќе ги пронајдат, а потребите се разликуваат од една операција до друга. Сметководствените табели се корисни за запишување на основните информации за многубројни извори; споделувани папки што се чуваат во „облак“ (cloud-based) се корисни за чување на големи количества снимки од прикази на екран. (Ако има потреба од чување на снимки на екран, од витално значење е на документот веднаш да му дадете препознатливо име: Нема многу нешта што се поиритантни од обидот да откриете кој од 100 документи насловени „Screenshot“ е тој што ви треба.) Текстуални документи се добри за чување на мешавина од информации, но брзо стануваат презаситени и незгодни за ракување ако се работи за голема операција.

Каков и формат да изберете, некои информации секогаш треба да бидат зачувани. Тие информации вклучуваат како бил пронајден изворот (клучна точка), неговото име и УРЛ адреса, датумот на создавање (ако е познат), и бројот на следбеници, следења, допаѓања и/или прегледи. Основните информации вклучуваат и основен опис на изворот (на пример, „про-саудиска сметка на арапски јазик со профилна фотографија од актерката Ема Вотсон (Emma Watson)), за да се потсетите за што се работи по прегледувањето на 500 други извори. Ако работите во тим, добро е да водите сметка кој член од тимот прегледал некој извор.

Линковите можат да се чуваат со користење на сервиси за архивирање како што се „Вејбек машин“ (Wayback Machine) или archive.is, но водете сметка дека архивите нема да ги објават корисниците што можеби несвесно влегле во интеракција со сомнителни извори, а исто така и дека архивираниот линк ги чува и визуелните елементи или направете снимка на екранот за секој случај. Осигурете се дека сите извори се зачувани на заштитени локации, на пример, документи заштитени со лозинка или шифрирани сефови. Внимавајте кој има пристап до нив и редовно ревидирајте го пристапот.

Конечно, добро е на изворите да им доделите оценка за веродостојност. Операциите за влијание често се потпираат на несвесни корисници за засилување на нивните содржини: тоа, всушност, најчесто е поентата на нивното дејствување. Колку сте сигурни дека најновиот извор е дел од операцијата и зошто? Нивото на веродостојност (високо, умерено или ниско) треба да се означи како одвоена ставка во табелата, а причините (разгледани подолу) треба да се додадат како забелешка.

Атрибуција и веродостојност

Најголем предизвик во идентификувањето на информативна операција е нејзината атрибуција на специфичен актер. Во многу случаи прецизната атрибуција ќе биде надвор од досегот на истражувачите на отворени извори. Најдоброто што може да се постигне е одреден степен на увереност дека операцијата веројатно ја води одреден актер, или дека различни извори припаѓаат на одредена операција, но утврдувањето кој стои зад неа ретко е можно со користење на отворени извори.

Информации како што се регистрации на интернет, IP адреси и телефонски броеви можат да обезбедат цврста атрибуција, но тие често се скриени за сите освен за платформите на социјалните медиуми. Токму затоа контактите со релевантните платформи се клучен дел

од истражувачката работа. Бидејќи платформите ги зголемија своите внатрешни истражни тимови, станаа поподготвени да понудат јавна атрибуција на информативните операции. Најцврстите атрибуции во неколку недамнешни случаи дојдоа директно од платформите, на пример, кога Твитер ги разоткри државните информативни операции на Кина што го таргетираа Хонгконг, и разоткривањето на операциите поврзани со владата на Саудиска Арабија од Фејсбук.

Индициите во содржината можат да имаат важна улога. На пример, една операција на Инстаграм откриена во октомври 2019 година постираше „мимови“ што беа скоро идентични со „мимовите“ поставени од руската Агенција за истражување на интернет, но без водените жигови на Агенцијата. Единствен начин за подготовка на тие „мимови“ е да се дојде до изворот на оригиналните слики што служеле како основа за постовите на Агенцијата и реконструкција на мимовите врз нив. Иронично, овој обид за маскирање на потеклото на постовите на Агенцијата сугерира дека изворот фактички е Агенцијата за истражување на интернет.

Слично, една голема мрежа од навидум независни интернет страни повторено поставуваше статии копурани, без наведување на авторите, од владини извори од Иран. Шемата беше толку репетитивна што се покажа дека тоа всушност е главната активност на тие интернет-страни. Тоа значеше дека е можно да се припише операцијата на про-ирански актери, но не беше можно дополнително да се утврди дали зад неа стои токму владата на Иран.

Во крајна линија, атрибуцијата е прашање на самоконтрола. Истражувачот треба да замисли дека е прашан, „како можеш да докажеш дека оваа операција е водена од лицето што го обвинуваш?“ Ако не може да си го одговори тоа прашање со сигурност, треба да се воздржи од изрекување на обвинувања. Идентификацијата и разоткривањето на информативни операции е тешка но значајна задача, а обидите тие да се припишат некому без солидна основа и на неточен начин, може да поткопа сè што сте направиле претходно.

11а. Студија на случај: Атрибуцијата во случајот „Бескрајна мајска мушичка“ (Endless Mayfly)

Автор: Габриела Лим

Габриела Лим *(Gabrielle Lim) е истражувач во Проектот за технологии и општествени промени (Technology and Social Change - TaSC) на Шоренстајн центарот на Кенедиевата школа на Универзитетот Харвард, и соработник на „Ситизен Лаб“ (Citizen Lab). Таа ги проучува влијанијата на цензурата и медиумските манипулации врз безбедноста и човековите права.*

Во април 2017 година, на Редит беше поставена неавтентична статија што го пародираше британскиот дневен весник „Индепендент“ (The Independent). Статијата содржеше измислен цитат од поранешниот заменик премиер на Британија Ник Клег (Nick Clegg) кој вели дека тогашната премиерка Тереза Меј (Theresa May) „им се додворува на арапските режими“. Искусните уредници на Редит (Redditors - редитори) веднаш посочија дека постот е сомнителен и лажен. Не само што беше хостиран на independent.co а не на www.independent.co.uk, туку оригиналниот објавувач беше „плитка персона“ што и претходно имаше поставено неколку неавтентични статии на Редит.

Поаѓајќи од таа неавтентнична статија, име на домен и персона, истражувачите во „Ситизен лаб“ во следните 22 месеци ја следеа и истражуваа мрежата што стои зад таа повеќестрана информативна операција на интернет. Именувана „Бескрајна мајска мушичка“ (Endless Mayfly), целта на операцијата беше да ги таргетира новинарите и активистите преку неавтентични интернет страни, со пародирање на интернет страните на етаблирани медиуми и ширење на лажни и информации што предизвикуваат поделби во општеството.

Општо говорејќи, мрежата пародира почитуван информативен медиум во неавтентична статија, засилувајќи ја преку мрежа од интернет страни и лажни „Твитер-персони“, а потоа или ќе ја избрише или ќе ја пренасочи неавтентичната статија откако таа ќе направи врева на интернет. Следниот пример прикажува пародирана статија замаскирана како да потекнува од Bloomberg.com, со погрешна адреса Bloomberq.com:

На сликата се прикажани две лажни онлајн-персони поврзани со Endless Mayfly кои твитуваат линк до копија на турскиот медиум „Дејли сабах“ (Daily Sabah). Забележете дека персоната десно, „jolie prevoit” користи профилна фотографија од актерката Елиша Катберт (Elisha Cuthbert).

До моментот на објавување на нашиот извештај во мај 2019 година, сетот на податоци со кои располагавме вклучуваше 135 неавтентични статии, 72 домени, 11 персони, една лажна организација и про-иранска мрежа издавачи што ги засилуваше лажните информации од неавтентичните статии. На крај заклучивме со умерена сигурност дека „Бескрајната мајска мушичка“ е информативна операција поврзана со Иран.

„Бескрајната мајска мушичка“ илустрира како можете да комбинирате анализа на мрежи и наративи со надворешно известување за да дојдете до утврдување на авторството. Таа, исто така, ги нагласува тешкотиите при припишувањето на информативните операции на одреден актер, зошто се потребни повеќе показатели, и како да се користи нивото на сигурност во наодите за да посочите колку сте сигурни во точноста на атрибуцијата.

Во крајна линија, атрибуцијата е тешка задача, често ограничена од несовршените информации со кои располагате, освен ако не успеете да извлечете признание од авторот или да обезбедите несоборливи докази. Поради тоа, припишувањето на авторството во многу случаи на медиумски манипулации често се изразува како проценка на веројатноста.

Триангулација на бројни податоци и анализи

Поради тајноста на информативните операции, способноста на актерите за влегување во кампањи за „лажно означување и предупредување“ и ефемерноста на доказите, атрибуцијата треба да биде резултат на комбинација од анализа и материјални докази. Во случајот на „Бескрајната мајска мушичка“ заклучивме со умерена сигурност дека се работи за информативна операција поврзана со Иран поради показателите изведени од три видови на анализа:

1. Анализа на наративи
2. Анализа на мрежи
3. Надворешно известување и анализа

1. Анализа на наративи

Со дискурзивна и анализа на содржината на 135 неавтентични статии собрани во процесот на истражување, заклучивме дека промовираните наративи се усогласени со интересите на Иран. Сите статии беа кодирани во категории, а за категоризацијата одлучувавме по првото читање на сите статии. Беа спроведени два круга на кодирање: Во првиот круг, кодирањето го спроведова два истражувачи, независно еден од друг, а втората рунда беше спроведена заеднички од двајцата истражувачи за да се разрешат несогласувањата во кодирањето. Следната табела ги прикажува резултатите од процесот на кодирање.

Категорија	Број на статии	Опис на категоријата
Геополитички раздор	63 (46,7%)	Статијата опишува настани, дејства или изјави на владини претставници насочени кон странска држава што можат да се сметаат за провокативни, непријателски или противни на интересите на странската држава.
Домашен раздор	16 (11,9%)	Статијата опишува настани, дејства или изјави на политички актери што можат да сејат раздор помеѓу политичките партии или актери во една држава.
Соработка со Израел	14 (10,4%)	Статијата опишува настани, дејства или исјави на политички актери или владини претставници што прикажуваат соработка помеѓу Израел и друга држава.
Саудиска Арабија го поддржува тероризмот	9 (6,7%)	Статијата опишува настани, дејства или изјави што или ја поврзуваат Саудиска Арабија со терористички активности или посочуваат дека Саудиска Арабија го поддржува тероризмот.
Друго	5 (3,7%)	Статијата не влегува во ниту една категорија.
Не е архивиран	31 (23%)	Статијата не може да биде кодирана затоа што веќе не постои не нема „кеширана“ верзија, снимка од екран или копија од текстот што би овозможила каква било смислена анализа.
Копија од постоечка статија	5 (3,7%)	Статијата е директна копија од веќе постоечка реална статија.

По кодирањето на сите статии, можевме да ги утврдиме најчестите наративи промовирани од „Бескрајната мајска мушичка“. Ги споредивме со прелиминарните истражувања за регионот. Споредбата вклучуваше обемно истражување за разбирање на ривалствата и сојузите во регионот, геополитичките интереси и закани, како и историјата на контрола на информирањето. Тоа беше потребно за контекстуализација на доказите и сместување на наративите во поширокиот политички контекст. Знаејќи ги резултатите од кодирањето, утврдивме дека наративите најверојатно им служат на интересите на Иран.

2. Анализа на мрежи

Анализа на мрежа беше спроведена за да утврдиме кои домени или платформи се одговорни за амплифицирање на содржините. Кај „Бескрајна мајска мушичка“, во ширењето на неавтентичните статии и лажните информации во нив беа вклучени две мрежи: мрежа од про-ирански интернет страни и група на про-ирански персони на Твитер. Двете мрежи фигурираа во атрибуцијата на „Бескрајната мајска мушичка“ затоа што постојано туркаа приказни на линија со официјалните политики, јавни изјави и ставови на Иран во врска со Саудиска Арабија, Израел и САД.

Мрежа на издавачи - Мрежата се состоеше од повеќе навидум про-ирански интернет страни што се претставуваа како независни информативни медиуми. Вклупно пронајдовме 353 интернет страници на 132 домени што ги наведуваа или ставаа линкови до неавтентичните статии на „Бескрајната мајска мушичка“. Процесот вклучуваше пребарување на Гугл на УРЛ адресите и насловите на сите неавтентични статии. Дополнително, ги прегледавме и линковите твитувани од персоните во мрежата за идентификација на интернет страните што содржеа референци или линкови до статиите.

По тој процес, идентификувавме водечки 10 домени што најчесто се реферираа на неавтентичните статии. Од тие 10 домени, осум споделуваа исти АјПи адреси и податоци за регистрацијата, што укажуваше дека можеби се контролирани од ист актер. Содржината на тие интернет страни беше насочена кон промоција на иранските интереси. На пример, „ИУВМ Прес“ (IUVM Press) со 57 линкувања или референци на неавтентичните статии на „Бескрајната мајска мушичка“, содржи ПДФ документ насловен „Статут“ што експлицитно изјавува дека страната е против „активностите и проектите на државите на глобалната ароганција, империјализмот и Ционизмот“ (“the activities and projects of global arrogance states, the imperialism and Zionism”) и дека „Централата на Унијата е лоцирана во Техеран, главниот град на Исламската Република Иран“ (“The headquarters of the Union is located in the Tehran – capital of Islamic Republic of Iran”).

Мрежа од персони - Слично како и неавтентичните статии и мрежата на издавачи, персоните поврзани со „Бескрајната мајска мушичка“ на Твитер одлучно беа критички настроени кон Саудиска Арабија, Израел и западните држави воопшто. Анализата на нивните активности на Твитер утврди дека тие сметки промовираа комбинација од веродостојни и неавтентични статии што содржеа остра критика за политичките ривали на Иран. Да ја разгледаме, на пример, сметката на Твитер на „Заедница за мир, безбедност, правда“ („Peace, Security, Justice Community“), лажна организација идентификувана од нашата истрага. Не само што промовираше содржини насочени против Саудиска Арабија, Израел и САД, туку и профилната и насловната слика ја таргетираа Саудиска Арабија. Забележете го снајперскиот нишан преку Саудиска Арабија во профилната слика, како и мапата користена во насловната слика. Биографските податоци за сметката исто така посочуваат на Саудиска Арабија и вахабистичката идеологија како причинители на екстремизмот.

На сличен начин, следниот твит од една друга персона од „Бескрајна мајска мушичка“, „Мона А. Рахман“ (Mona A. Rahman) го спомнува новинарот и критичар на Саудиска Арабија Али ал-Ахмед (Ali al-Ahmed) во критиката на саудискиот престолонаследник Мохамед бин Салман (Mohammad bin Salman).

3. Надворешно известување и анализа

Ги споредивме нашите наоди и со известувањето на други субјекти. По дојавата од „ФајрАј“ (FireEye) во август 2018 година, на пример, Фејсбук деактивираше неколку сметки и страници поврзани со мрежата на издавачи користена од „Бескрајна мајска мушичка“.

Во својата анализа, „ФајрАј“ идентификуваше неколку домени што беа дел од мрежата на издавачи што ја откривме, како што се institutomanquehue.org и RPFront.com. И тие заклучија со умерена сигурност дека „сомнителната операција за стекнување влијание потекнува од Иран. Во своето известување за јавноста, Фејсбук исто така забележа дека операцијата најверојатно потекнува од Иран.

Дополнително, Твитер објави сет на податоци за сметки поврзани со Иран што биле суспендирани поради „координирани манипулации“. Иако во времето на суспензијата сметките со помалку од 5,000 следбеници беа анонимизирани, успеавме да идентификуваме една персона од „Бескрајна мајска мушичка“ (@Shammari_Tariq) од сетот на податоци на Твитер. Проценките на Твитер, Фејсбук и „ФајрАј“ беа корисни во потврдувањето на нашата претпоставка затоа што обезбедија докази што не беа дел од нашите напори за собирање податоци, и се поклопуваа со субјектите на „Бескрајна мајска мушичка“ што ги идентификувавме. На пример, анализата на „ФајрАј“ идентификуваше телефонски броеви и регистрациски информации поврзани со сметките на Твитер и домените поврзани со „Бескрајна мајска мушичка“ - доказ што не беше дел од нашиот сет на податоци.
Слично, Фејсбук и Твитер ги имаа на увид информациите за регистрација на сметките како што се АјПи адресите до кои немавме пристап. Дополнителните податоци во таквите надворешни извештаи помогнаа да ги збогатиме нашите докази.

Стигнување до умерена сигурност

Во случајот на „Бескрајна мајска мушичка“, доказите што ги собравме - про-иранските наративи, персони и мрежата на издавачи - посочуваше кон Иран како веројатен извор на информативната операција. Доказите потоа ги споредивме со веродостојните надворешни извештаи и истражувања спроведени од „ФајрАј“, Фејсбук и Твитер, и тие ги потврдија нашите наоди.

Секој индивидуален доказ, иако сам по себе недоволен за соодветна атрибуција, помогна да ја потврдиме и зацврстиме хипотезата во целина, а споредена со вкупните докази откриени од нашата истрага.

И покрај бројните показатели што посочуваа кон Иран, сè уште немавме дефинитивни докази. Користевме рамка за кибер-атрибуција што често се користи во разузнавачката заедница. Рамката користи повеќе индикатори и пробабилистичка увереност (ниска, умерена, висока), дозволувајќи им на истражувачите да ги прикажат наодите со квалификација за нивото на несигурност.

На крај заклучивме, со умерена сигурност во наодите, дека „Бескрајна мајска мушичка“ е операција поврзана со Иран, што според Канцеларијата на Директорот за разузнавање на САД (U.S. Office of the Director of National Intelligence) значи „информациите се потпираат на веродостојни извори но нивниот квалитет не е доволен, ниту се доволно потврдени за да добијат повисоко ниво на доверба“. Решивме да не избереме повисоко ниво на увереност затоа што чувствувавме дека нема доволно докази за целосно да се исклучи можноста дека се работи за операција за лажно означување и алармирање - значи, дека некој се труди да направи да изгледа дека Иран стои за целата операција - или трета страна со симпатии за иранските интереси.

Атрибуцијата на информативните операции како што е „Бескрајна мајска мушичка“ скоро секогаш ќе зависи од нецелосни и несовршени информации. Оттаму, доделувањето на ниво на доверба на наодите е значајна компонента од атрибуцијата - затоа што тоа бара огромна претпазливост. Неточната атрибуција или „напумпано“ ниво на доверба можат да имаат страшни последици, особено ако погрешната проценка доведе до нови владини политики за контра-мерки. За да се избегне праксата на избрзана и погрешна атрибуција, значајно е да се разгледаат повеќе показатели, видот на доказите и анализите, и да се употреби ниво на доверба што дозволува алтернативни хипотези или можност дека недостигаат некои податоци.

11б. Студија на случај: Истражување на информативна операција во Западна Папуа

Автори: Елиза Томас, Бенџамин Стрик

Бенџамин Стрик *(Benjamin Strick) е истражувач на отворени извори во БиБиСи, соработник на „Белингкет" и инструктор за техники за отворени извори, гео-просторно разузнавање и анализа на мрежи. Има претходно искуство на работа во областа на правото и во воените сили, а неговиот фокус е на користењето на ОСИНТ/ГЕОИНТ (разузнавање на отворени извори/гео-разузнавање), гео-локација и разузнавачки методи за добри цели, преку човекови права, конфликти и приватност.*

Елиза Томас *(Elise Thomas) е слободна новинарка и истражувачка што соработува со Меѓународниот центар за кибер политики (International Cyber Policy Centre) при Институтот за стратегиски политики од Австралија (Australian Strategic Policy Institute). Објавувала во „Вајрд" (Wired), „Форин полиси" (Foreign Policy), „Дејли бист" (The Daily Beast), „Гардијан" (The Guardian) и други публикации. Претходно работела и како помошник за уредувачки прашања во Канцеларијата на ОН за координација на хуманитарни прашања (UN Office for the Coordination of Humanitarian Affairs), и како пишувач и истражувач на подкасти.*

Во август 2019 година, повторно се разгореа сепаратистичките тензии во Западна Папуа, провинција што стана дел од Индонезија со една контроверзна одлука во 1960-те години. Од тој момент, регионот страда од раширени обвинувања за кршења на човековите права од индонезиските власти во обид да задушат секакво спротивставување.

Пристапот до регионот е ограничен, а имало случаи кога на странски новинари им било забрането да известуваат од покраината. Поради сето тоа, социјалните медиуми се клучен извор за следење и известување за состојбите во Западна Папуа.

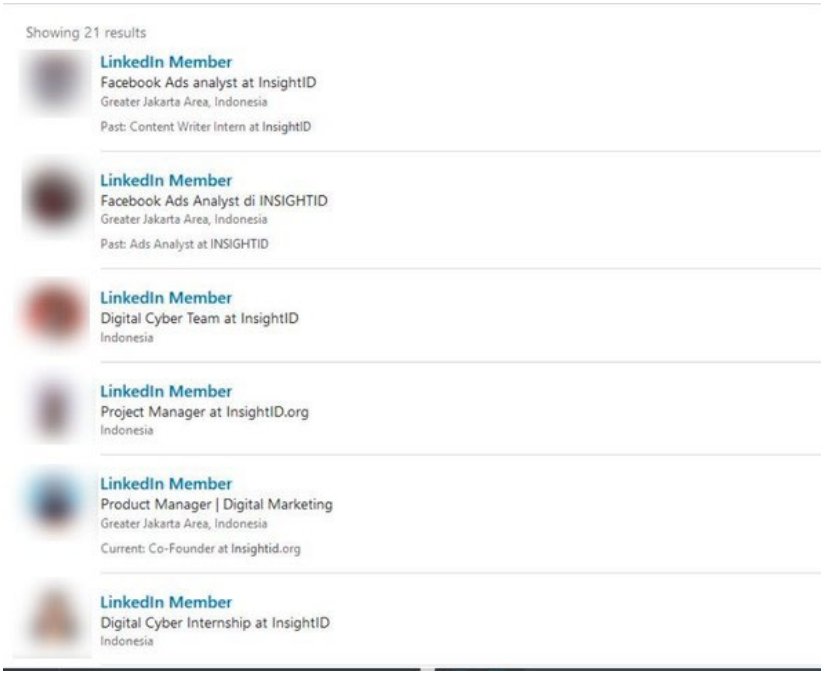
Во обидите да гео-лоцираме снимки за насилството во ФакФак (FakFak) што пристигнуваа до нас, некој во тимот идентификуваше два хаштагови што се шират на Твитер, #WestPapua и #FreeWestPapua.

Истражувањето на тие хаштагови откри цел бран на лажни сметки што автоматски постираат исти видеа и тектови со користење на хаштаговите. Сметките, исто така, разменуваа ретвитови и допаѓања меѓу себе, помагајќи во натамошното засилување и зголемен ангажман на тие хаштагови.

За анализата на автоматизираните сметки веќе говоревме во повеќе детали во Поглавјето 3. Врз основа на таа анализа, ја проширивме истрагата за да ги идентификуваме лицата или групите што стојат зад операцијата. Во тој процес, откривме слична, помала и навидум неповрзана кампања, а успеавме и да го идентификуваме одговорното лице зад кампањата. Операторите на двете кампањи на крај ја признаа својата инволвираност откако беа контактирани и прашани за тоа од БиБиСи.

Размерите на првата кампања и фактот што се одвиваше на повеќе платформи ни понуди низа можности да пронајдеме траги што би ги искористиле како стожерна точка за наоѓање повеќе информации за операторите на кампањата.

Првата корисна информација беа имињата на интернет страните споделувани од мрежата на сметки на Твитер и Фејсбук. Пребарувањата со „Whois“ откриja дека четири од домените се регистрирано со лажно име и лажна е-маил адреса, но со вистински телефонски број. Тој број го внесовме во ВотсАп (WhatsApp) за да видиме дали е поврзан со некоја корисничка сметка. Се покажа дека е поврзан а сметката имаше и профилна фотографија. Со реверзибилно пребарување на слики на Yandex ја поврзавме профилната слика со кориснички сметки на Фејсбук, ЛинкдИн и Freelancer.com. Преку соодветната сметка на ЛинкдИн можевме да го пронајдеме тогашното работно место на тоа лице и да видиме листа на негови колеги.



Лицето беше вработено во компанијата „ИнсајтИД“ (InsightID) од Џакарта која, според корпоративната интернет страна, нуди „интегрирани програми за односи со јавност и дигитален маркетинг“.

Собравме и дополнителни податоци и индикатори дека „ИнсајтИД“ е одговорна за информативната операција. На интернет страната, „ИнсајтИД“ ја наведуваше работата на „Иницијативата за развој на програми во Папуа“ (Papua Program Development Initiative), која „го истражува брзиот социо-економски развој во Папуа и ги разгледува предизвиците со кои се соочува тој развој“. Поранешни вработени и приправници во „ИнсајтИД“ опишаа дека производството на видео содржини, пишување текстови и превод на содржини било дел од работните задачи во склоп на развојниот проект во Папуа.

Еден поранешен вработен изјави на својот профил на ЛинкдИн дека нивните дела можеле да бидат видени на „Вест Папуан“ (West Papuan) (Instagram, Facebook, Website)“. „Вест Папуан“ беше една од петте информативни интернет страни вклучени во кампањата. Друг вработен во „ИнсајтИД“ креирал сметка на ЈуТјуб на свое име за поставување на видео како дел од кампањата. Видеото потоа било вградено (embed) во westpapuan.org.

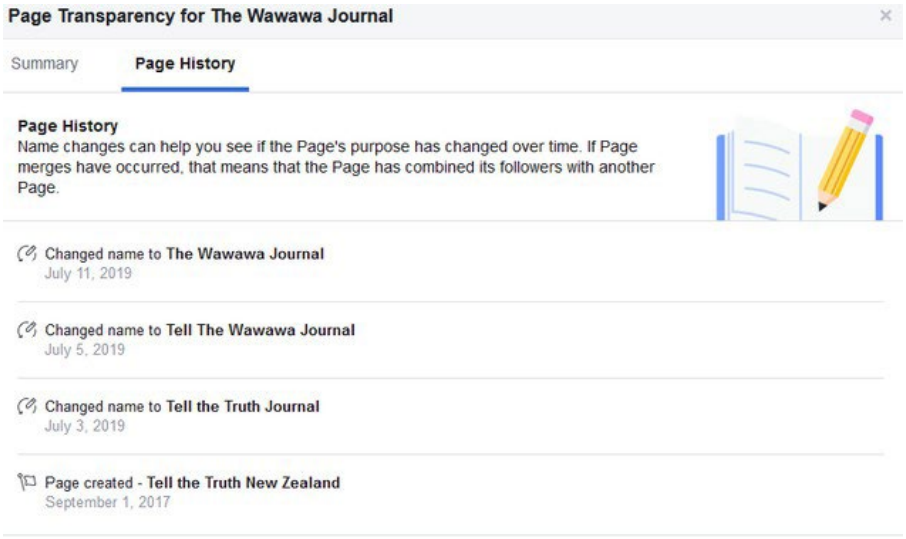
Дополнително пребарување на записите за доменот откриваат дека со-основачот на „ИнсајтИД“ ја користел корпоративната е-маил адреса за регистрација на 14 домени во еден ден, повеќето од нив јасно и директно поврзани со Западна Папуа. Меѓу нив се и домените westpapuafreedom.com, westpapuagenocide.com и westpapuafact.com. Секоја натамошна информација додаваше нови докази дека за операцијата е одговорен „ИнсајтИД“.

Во тој момент новинари на БиБиСи се обидоа да го контактираат „ИнсајтИД“ за да побараат коментар. Иако не добија одговор, „ИнсајтИД“ на крај ја призна својата одговорност, изјавувајќи во пост на социјалните медиуми дека „нашите содржини ја бранат Индонезија од измамничкиот наратив на сепаратистичките групи од Западна Папуа“.

Не успеавме да го идентификуваме клиентот што го ангажирал „ИнсајтИД“ да ја спроведе информативната кампања.

Откривајќи ја поголемата операција, истраживме и една помала мрежа од три интернет страни што се претставуваа како независни извори на вести со поврзани профили на социјалните медиуми. Иако навидум неповрзани со првата кампања, тие интернет страни ги таргетираа меѓународните перцепции за состојбата во Западна Папуа, со фокус на јавноста во Нов Зеланд и Австралија.

Клучот за идентификацијата на одговорното лице беше дека страницата на Фејсбук на еден од брендовите, „Вавава журнал“ (Wawawa Journal), изворно се викаше „Tell the Truth NZ“ (Кажи ја вистината Нов Зеланд). Тоа можевме да го видиме со преглед на историјата на именување на страницата. Тоа ни овозможи да ја поврземе со доменот tellthetruthnz.com, регистриран од Мухамед Росјид Јазули (Muhamad Rosyid Jazuli).



Во контакт со новинари на БиБиСи, Јазули призна дека е оператор на кампањата. Тој работи во „Џенгала центар“ (Jenggala Center), организација основана од потпретседателот на Индонезија Јусуф Кала (Jusuf Kalla). Организацијата е основана во 2014 година за промоција на неговиот реизбор и за поддршка на администрацијата на претседателот Јокови (Jokowi).

Оваа истрага покажува дека идентификацијата на информативните кампањи и атрибуцијата на одговорните лица и групи не бара нужно употреба на сложени техники или алатки - но секако бара трпение и доза среќа. Истрагата се потпираше на отворени извори како што се архивите „Whois“, реверзибилно пребарување слики, профили на социјалните медиуми и анализа на изворните кодови на интернет страни. Фактот што кампањате се одвиваше на повеќе платформи, во комбинација со профилите на социјалните медиуми и на ЛинкдИн на вработени во „ИнсајтИД“, беше клучен за да можеме да составиме толку многу мали траги и да ја насликаме поширокаата слика.

Ако треба да извлечеме клучна лекција научена од овој пример, нека биде дека треба да се размисли за тоа како можете да ги искористите деталите или знаците од една платформа за да се насочите кон друга.

За изданието

„Verification Handbook 3 - For Disinformation and Media Manipulations»
Edited by Craig Silverman
European Journalism Centre, 2019

Уредник: **Крег Силверман**
Уредник консултант: **Клер Вордл**
Уредник на текст: **Мерил Перлман**

Автори на текстовите: **Бен Колинс, Бен Нимо, Бенџамин Стрик, Бренди Задрозни, Шарлот Годар, Клер Вордс, Крег Силверман, Дони О'Саливен, Елиза Томас, Фарида Вис, Габриела Лим, Џема Багајаја-Мендоза, Хана Гај, Хенк ван Ес, Џејн Литвиненко, Џоан Донован, Џоана Вајлд, Сем Грегори, Сержиу Литке, Сајмон Фокнер, Вернис Тантуко**

Менаџер на издание: **Арне Граулс**

Книгата е издание на Европскиот новинарски центар (European Journalism Centre), и нејзиното издавање беше овозможено од финансиската помош од „Крег Њумарк Филантропис“ (Craig Newmark Philanthropies.