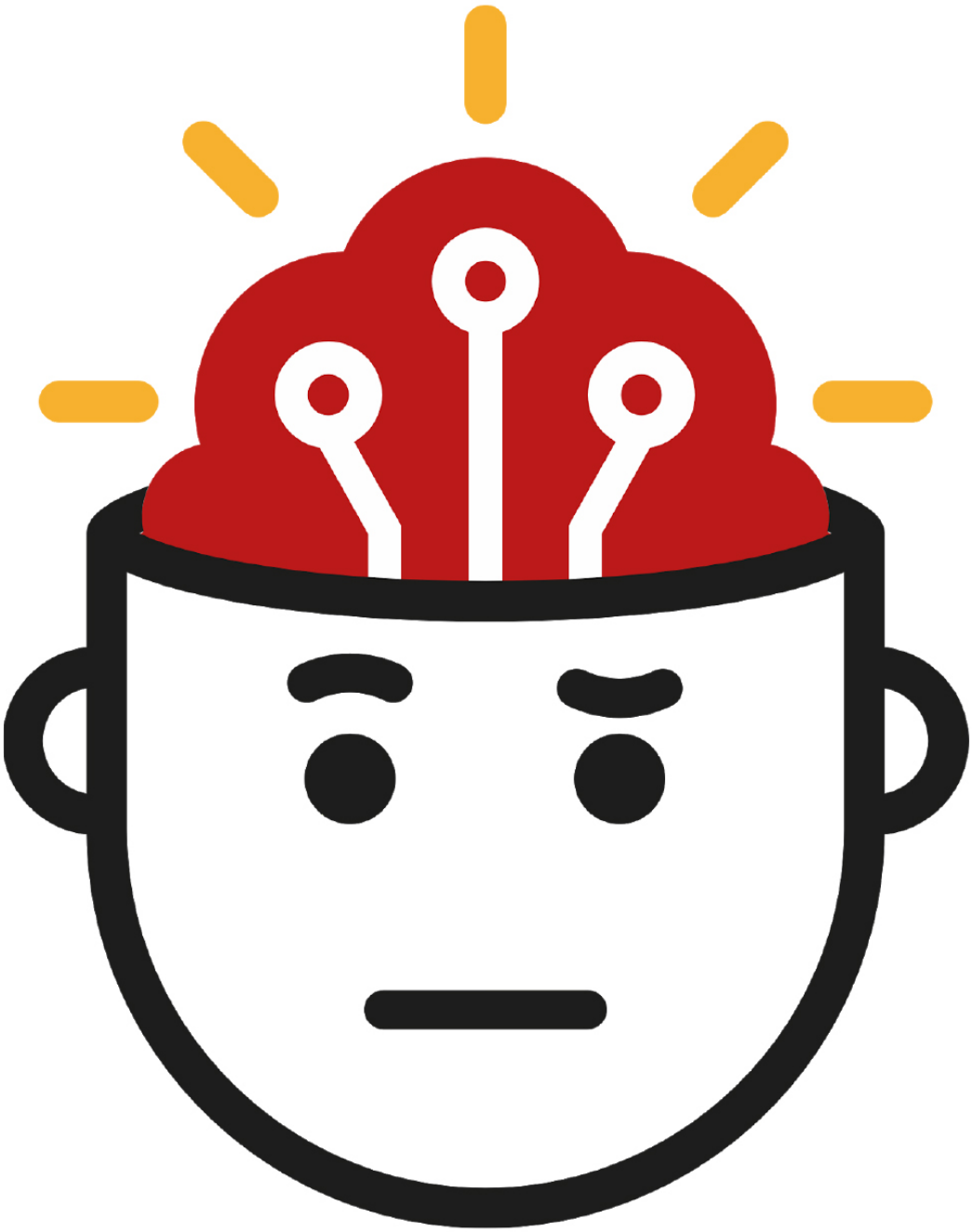
Doracak i verifikimit

Për dezinformata dhe manipulime mediatike

Udhëzues përfundimtar për hulumtimin e platformave dhe llogarive në internet për të zbuluar aktivitetin joautentik dhe përmbajtjet e manipuluara



Redaktuar nga Kreg Silvermen

Botimin e Doracakut për verifikimin e dezinformatave dhe manipulimeve mediatike e përgatiti
Qendra për Zhvillimin e Mediave nga Shkupi

ЦЕНТАР за РАЗВОЈ на МЕДИУМИ

Ky projekt është i mbështetur me grant nga Ambasada e SHBA-ve. Mendimet, zbulimet dhe konkluzionet ose rekomandimet e paraqitura këtu janë të implementuesve/ autorëve dhe nuk i reflektojnë domosdoshmërisht ato të Qeverisë së SHBA-ve

Përkthimi në gjuhën shqipe: Petrit Saraçini
Redaktor teknik: Ljuben Dimanovski

Shkurt 2024

KAPITUJT

Hulumtimi i dezinformatave dhe manipulimeve mediatike

Shkruan: Kreg Silvermen

Kreg Silvermen *(Craig Silverman) është redaktor mediatik i BuzzFeed News, ku drejton ritmin global që mbulon platformat, keqinformimin onlajn dhe manipulimet mediatike. Ai më parë ka redaktuar "Doracakun e verifikimit" dhe "Doracakun e verifikimit për raportimin hulumtues", dhe është autor i "Gënjeshtrat, gënjeshtrat e mallkuara dhe përmbajtja virale: Si uebfaqet e lajmeve përhapin (dhe përgënjeshtrojnë) thashethemet në internet, pretendimet e paverifikuara dhe informatat e gabuara (misinformatat)."*

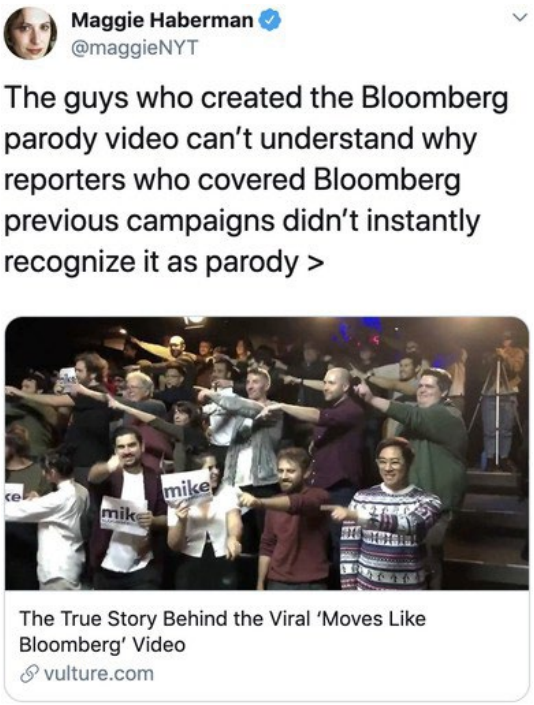
Në dhjetor të vitit 2019, përdoruesi i Twitter @NickCiarelli shpërndau një video për të cilën tha se tregonte një rutinë vallëzimi që po adoptohej nga mbështetësit e fushatës presidenciale të Majkëll Blumbergut. Entuziazmi dhe koreografia e dobët e videos e ndihmuan menjëherë atë për të grumbulluar rituite dhe pëlqime, kryesisht nga njerëz që kënaqeshin ta tallnin. Videoja përfundimisht tërhoqi më shumë se 5 milionë shikime në Twitter.

Biografia e Ciarellit në Twitter thoshte se ai ishte një praktikant për fushatën e Blumbergut dhe postimet e tij të mëvonshme përfshinin pika provuese, si një skrinshot (pamje ekrani e ruajtur në kompjuter) të një e-maili nga një punonjës i supozuar i fushatës së Blumbergut që gjoja miratonte buxhetin për videon.

Por një kërkim i shpejtë në Google për emrin e Ciarellit tregoi se ai është një komedian që ka krijuar video humori në të kaluarën. E, ai e-maili nga punonjësi i Blumbergut? Ai ishte i dërguar nga partneri i shpeshtë komik i Ciarellit, Brad Evans. Edhe ky informacion mund të gjendej vetëm me një kërkim në Google.

Por në minutat dhe orët e para, disa besuan se videoja që mund të cilësohet si krinxh ishte një produksion zyrtar i Blumbergut.

Megi Haberman, një reportere e njohur politike e New York Times, shkroi në Twitter se gazetarët që kanë mbuluar fushatat e mëparshme të Blumbergut për kryebashkiak kishin arsye për të mos e hedhur poshtë atë menjëherë:



Dituria mund të marrë shumë forma, e në këtë mjedis të ri digjital, gazetarët duhet të jenë të kujdesshëm për të mos u mbështetur shumë në çdo burim të caktuar informacioni – bile edhe nëse është përvojë e tyre e drejtpërdrejtë.

Me sa duket, disa reporterë që e njihnin Blumbergun dhe stilin e tij të fushatës menduan se kjo video mund të ishte e vërtetë. Në të njëjtën kohë, gazetarët që nuk dinin asgjë për Blumbergun dhe zgjodhën ta vlerësojnë videon sipas burimit të saj, mund të kishin gjetur menjëherë përgjigjen e saktë - në këtë rast, thjesht duke kërkuar në Google emrin e njeriut që e shpërndau atë.

Poenta nuk është se përvoja rreth mbulimit të Blumbergut është e keqe. Poenta është se në çdo moment mund të drejtohemi në rrugë të gabuar nga ajo që mendojmë se dimë. E në disa raste, baza jonë e njohurive dhe përvojës mund të jetë edhe negative. Gjithashtu mund të mashtrohemi nga sinjalet digjitale si rituitet dhe shikimet, ose nga përpjekjet për t'i manipuluar ato.

Siç tregoi videoja e Blumbergut, duhet pak përpjekje për të krijuar sinjale mashtruese si një biografi në Twitter ose një skrinshot i një e-maili që duket se mbështet përmbajtjen dhe pretendimin. Nga ana tjetër, këto gjëra ndihmojnë që përmbajtja të bëhet virale. Dhe, sa më shumë rituite dhe pëlqime grumbullohen, aq më shumë këto sinjale do të bindin disa se videoja mund të jetë e vërtetë.

Natyrisht, ka shembuj shumë më mashtrues se ky. Ndryshe nga Ciarelli, njerëzit që qëndrojnë pas operacioneve të informacionit dhe fushatave të dezinformimit rrallë e zbulojnë mashtrimin. Por, ky rast studimi tregon se sa konfuze dhe frustruese është për të gjithë, përfshirë gazetarët, të lundrosh në një mjedis informacioni të mbushur me sinjale cilësie dhe besimi lehtësisht të manipulueshme.

Besimi është themeli i shoqërisë. Ai informon dhe lubrifikon të gjitha transaksionet dhe është kyç për lidhjet dhe marrëdhëniet njerëzore. Por është e rrezikshme të operosh me besim të paracaktuar në mjedisin tonë digjital.

Nëse parazgjedhja juaj është të besoni se llogaritë në Twitter që rituitojnë një video po e amplifikojnë atë në mënyrë organike, do të viheni në lojë. Nëse besoni se komentet për një produkt janë të gjitha nga klientë të vërtetë, do t'i humbni paratë tuaja. Nëse besoni se çdo artikull lajmesh në news feed-in (kronologjinë e lajmeve) tuaj përfaqëson një koleksion të paanshëm të asaj që keni më shumë nevojë të shihni, do të përfundoni të keqinformuar.

Është e rëndësishme që çdo person ta njohë këtë realitet, por për gazetarët kjo është thelbësore. Ne jemi në shënjestër të fushatave të koordinuara dhe të mirë-financuara për të tërhequr vëmendjen tonë, për të na mashtruar që të amplifikojmë mesazhe dhe për të na përkulur ndaj vullnetit të shteteve dhe forcave të tjera të fuqishme.

Lajmi i mirë është se kjo krijon një mundësi - dhe domosdoshmëri - për hetim.

Ky doracak bazohet në njohuritë dhe përvojën e gazetarëve dhe studiuesve të shquar për të ofruar udhëzime se si të ekzekutohen hulumtimet e manipulimeve të mediave digjitale, dezinformatave dhe operacioneve të informacionit.

Po veprojmë në një ekosistem informacioni kompleks dhe me zhvillim të përshpejtuar. Kërkon një qasje po aq në zhvillim të ndërtuar mbi testimin e supozimeve tona, gjurmimin dhe parashikimin e kundërshtarëve dhe zbatimin e teknikave më të mira të hetimit me burim të hapur dhe teknikave tradicionale të raportimit. Dobësitë në botën tonë digjitale të drejtuar nga të dhënat kërkojnë që gazetarët të vënë në dyshim dhe të shqyrtojnë çdo aspekt të saj dhe të zbatojnë aftësitë tona për të ndihmuar në drejtimin e publikut drejt informacionit të saktë dhe të besueshëm. Kjo gjithashtu kërkon që gazetarët të mendojnë se si mund t'u japim padashur oksigjen aktorëve të këqij dhe fushatave të krijuara për të na shfrytëzuar, dhe për të nxituar që të drejtohet gishti ndaj aktorëve shtetërorë kur provat nuk e mbështesin atë.

Qëllimi i këtij doracaku është t'i pajisë gazetarët me aftësitë dhe teknikat e nevojshme për ta bërë këtë punë në mënyrë efektive dhe të përgjegjshme. Ai gjithashtu ofron bazën bazë në teorinë, kontekstin dhe mentalitetin që u mundëson gazetarëve të ofrojnë punë me cilësi të lartë që informon publikun, ekspozon aktorët e këqij dhe ndihmon në përmirësimin e mjedisit tonë të informacionit. Por gjëja e parë që duhet kuptuar është se njohuritë dhe mjetet praktike janë të padobishme nëse nuk i qaseni kësaj pune me mendësinë e duhur.

Kjo do të thotë se duhet kuptuar se gjithçka në mjedisin digjital mund të luhet dhe manipulohet, dhe të njihet shumëllojshmëria e gjerë të njerëzve dhe subjekteve me nxitje për ta bërë këtë. E bukura e këtij mjedisi është se ka shpesh, edhe pse jo gjithmonë, një gjurmë të dhënash, ndërveprimesh, lidhjesh dhe "thërrimeve të bukës" të tjera digjitale për t'u ndjekur. Dhe shumë prej tyre mund të jenë të disponueshme publikisht nëse di se ku dhe si të kërkosh.

Hetimi në botën digjitale do të thotë të mos marrësh asgjë në vlerën që paraqitet. Do të thotë të kuptosh se gjërat që duken të jenë të matshme dhe të drejtuara nga të dhënat - pëlqimet, shpërndarjet, rituitet, trafiku, rishikimet e produkteve, klikimet në reklama - manipulohen lehtësisht dhe shpesh. Do të thotë të pranosh që gazetarët janë fokusi kryesor i manipulimit të medias dhe operacioneve të informacionit, si në aspektin e të qenit në shënjestër dhe të sulmuar, si dhe të shihen si një kanal kyç për përhapjen e keqinformimit dhe dezinformimit. Dhe kjo do të thotë të pajisësh veten dhe kolegët me mentalitetin, teknikat dhe mjetet e nevojshme për t'u siguruar se po ofroni informacione të besueshme dhe të sakta - e jo për të përforcuar të pavërtetat, përmbajtjet e manipuluara ose troll fushatat.

Në thelb të mentalitetit është paradoksi i hulumtimit digjital: Duke mos besuar asgjë në fillim, ne mund të angazhohemi në punë që zbulon ato që duhet dhe nuk duhet t'i besojmë. E kjo na mundëson të prodhojmë përmbajtje që komunitetet të cilave u shërbejmë janë të gatshme dhe në gjendje t'i besojnë.

Së bashku me këtë, ka disa baza që do t'i shihni të theksuara në mënyrë të përsëritur në kapitujt dhe studimet e rasteve:

- *Mendoni si një kundërshtar.* Çdo veçori e re e një platforme ose shërbimi digjital mund të shfrytëzohet në një farë mënyre. Është e rëndësishme të vini veten në vendin e dikujt që kërkon të manipulojë mjedisin për arsye ideologjike, politike, financiare ose të tjera. Kur shikoni përmbajtjen dhe mesazhet digjitale, duhet të merrni parasysh motivet që nxisin krijimin dhe përhapjen e saj. Është gjithashtu thelbësore të jeni në rrjedhë me teknikat më të fundit që përdoren nga aktorët e këqij, tregtarët digjitalë dhe të tjerë, mbijetesa e të cilëve mbështetet në gjetjen e mënyrave të reja për të fituar vëmendje dhe për të fituar të ardhura në mjedisin digjital.
- *Përqendrohuni te aktorët, përmbajtja, sjellja dhe rrjetet.* Qëllimi është të analizohen aktorët, përmbajtja dhe sjellja dhe se si ata dokumentojnë se si mund të punojnë njëzëri si rrjet. Duke i krahasuar dhe vënë në kontrast këto katër gjëra me njëra-tjetrën, mund të filloni të kuptoni atë që po shihni. Siç do ta shihni në kapituj të shumtë dhe studime të rasteve, një qasje themelore është të filloni me një pjesë të përmbajtjes ose një entitet të tillë si një uebfaqe dhe të përqendroheni në të për të identifikuar një rrjet më të madh përmes sjelljes dhe lidhjeve të tjera. Kjo mund të përfshijë ekzaminimin e rrjedhës së përmbajtjes dhe aktorëve nëpër platforma të ndryshme, e herë pas here edhe në gjuhë të ndryshme.
- *Monitoroni dhe grumbulloni.* Mënyra më e mirë për të identifikuar manipulimin dhe dezinformimin mediatik është ta kërkosh atë gjatë gjithë kohës. Monitorimi dhe gjurmimi i vazhdueshëm i aktorëve të njohur, temave dhe komuniteteve të interesit është thelbësor. Ruani dhe organizoni atë që gjeni, qoftë në fletëllogaritëse (spreadsheet), folderë(dosje në kompjuter) të skrinshoteve ose duke përdorur mjete me pagesë si Hunchly.
- *Kini kujdes me atribuimin.* Ndonjëherë është e pamundur të thuhet saktësisht se kush qëndron pas një llogarie të caktuar, ndonjë përmbajtjeje ose një operacioni më të madh të informacionit. Një arsye është se aktorët me motive të ndryshme mund të sillen në mënyra të ngjashme dhe të prodhojnë ose të amplifikojnë të njëjtin lloj përmbajtjeje. Edhe vetë platformat – të cilat kanë qasje shumë më të mirë në të dhëna dhe më shumë burime – bëjnë gabime në atribuim. Provat më të suksesshme dhe bindëse zakonisht kombinojnë provat digjitale me informacionin nga burimet e brendshme - një përzierje ideale e punës hulumtuese në internet dhe asaj tradicionale. Kjo po bëhet edhe më e vështirë përderisa aktorët shtetërorë dhe të tjerët evoluojnë dhe gjejnë mënyra të reja për të fshehur gjurmët. Atribuimi është i vështirë; gabimi në atribuim do të dëmtojë të gjithë punën e kujdesshme që ka çuar deri në të.

Së fundi, një shënim për dy doracakët që i paraprinë këtij botimi. Kjo punë bazohet në themelet e botimit të parë të Manualit të Verifikimit dhe Manualit të Verifikimit për Raportimin Hulumtues. Secili prej tyre ofron shkathtësi themelore për monitorimin e mediave sociale, verifikimin e imazheve, videove dhe llogarive të mediave sociale dhe përdorimin e motorëve të kërkimit për të identifikuar njerëzit, kompanitë dhe subjektet e tjera.

Shumë nga kapitujt dhe studimet e rasteve në këtë doracak janë shkruar me supozimin se lexuesit zotërojnë njohuritë bazë të paraqitura në këto botime të mëparshme, veçanërisht në doracakun e parë. Nëse keni vështirësi për ta ndjekur, ju inkurajoj të filloni me doracakun e parë.

Tani, t'ia nisim punës.

Epoka e çrregullimit të informacionit

Shkruan: Kler Uordëll

Kler Uordëll *(Claire Wardle) e udhëheq drejtimin strategjik dhe kërkimin për First Draft, organizatë jofitimprurëse globale që mbështet gazetarët, shkencëtarët dhe teknologët që punojnë për të adresuar sfidat në lidhje me besimin dhe të vërtetën në epokën digjitale. Ajo ka qenë bursiste e Qendrës Shorenstein për Media, Politikë dhe Politika Publike në Shkollën Kennedy të Harvardit, Drejtoreshë e kërkimeve në Qendrën për Gazetari Digjitale në Shkollën Diplomike të Gazetarisë të Universitetit Columbia dhe drejtuese e mediave sociale për UNHCR, Agjencinë e Kombeve të Bashkuara për Refugjatë.*

Siç e dimë të gjithë, gënjeshtrat, thashethemet dhe propaganda nuk janë koncepte të reja. Njerëzit çdoherë e kanë pasur aftësinë të mashtrojnë, dhe ka disa shembuj të famshëm historik kur përmbajtja e fabrikuar është përdorur për ta çorientuar publikun, për të destabilizuar qeveritë ose për të rritur tregjet e aksioneve. Ajo që është e re tani është lehtësia me të cilën çdokush mund të krijojë përmbajtje të rreme dhe çorientuese që janë bindëse, si dhe shpejtësia me të cilën përmbajtja mund të qarkullojë nëpër botë.

E kemi kuptuar çdoherë që ka pasur kompleksitete në mashtrime. Një masë nuk i nxë të gjitha. Për shembull, një gënjeshtër e padëmshme ("gënjeshtër e bardhë") e thënë për të mbajtur paqe gjatë një zënke në familje nuk është e njëjtë sikurse një deklaratë çorientuese nga një politikan në përpjekje për të fituar më shumë vota. Një fushatë propaganduese e financuar nga shteti nuk është e njëjtë sikurse një teori konspirative mbi zbarkimin në Hënë.

Fatkeqësisht, gjatë viteve të fundit, çdo gjë që mund të bjerë në kategoritë e përshkruara këtu është etiketuar si "lajme të rreme" (fake news), një term i thjeshtë që ka marrë përmasa globale, shpesh pa nevojën e përkthimit.

Them fatkeqësisht, sepse është mjerueshëm joadekuat për të përshkruar kompleksitetin që po e shohim. Shumica e përmbajtjeve që janë mashtruese, në njëfarë mënyre, nuk maskohen si një lajm. Aty janë meme-t, videot, fotografitë (imazhet), apo aktivitetet e koordinuara në Twitter, YouTube, Facebook ose Instagram. Dhe, shumica e tyre nuk janë të rreme; janë çorientuese, ose shpeshherë, autentike, por të përdorura jashtë kontekstit.

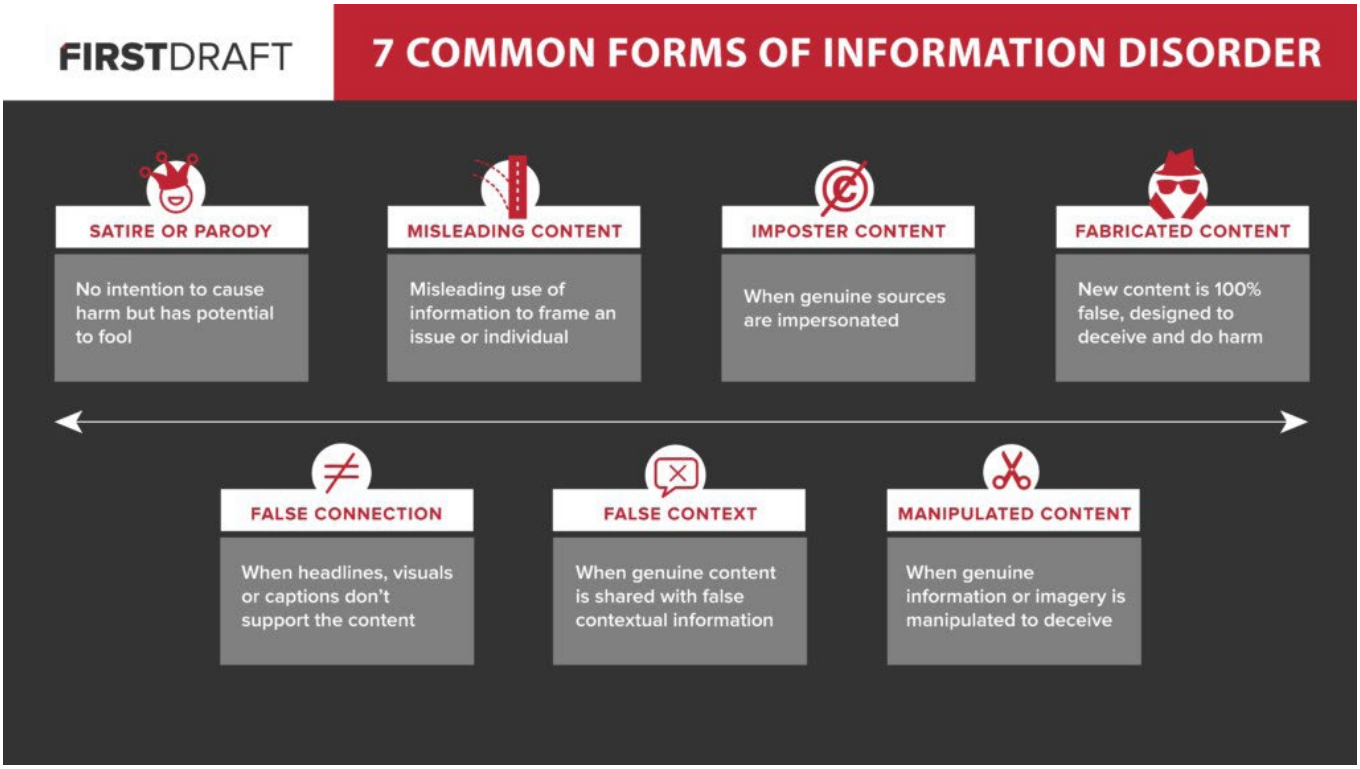
Dezinformata me ndikim më të madh është ajo që në të ka një thelb të së vërtetës: duke marrë diçka që është e vërtetë dhe duke e keqinterpretuar, apo duke e shpërndarë si diçka të re kur është realisht tri vite e vjetër.

Ndoshta më problematikja është që termi "lajme të rreme" është shndërruar në armë, kryesisht nga politikanët dhe përkrahësit e tyre për të sulmuar mediat profesionale informative anembanë botës.

Frustrimi im me këtë frazë më shtyu që ta krijoj termin "çrregullim i informacionit" me bashkautorin tim Husein Derakhshanin. Në vitin 2017 e shkruam një raport me titull "Çrregullim i informacionit", dhe i eksploruam sfidat e terminologjisë që ekziston mbi këtë temë. Në këtë kapitull, do t'i shpjegoj disa nga aspektet kyçe të definicioneve për ta kuptuar këtë temë, dhe për të folur në mënyrë kritike mbi të.

7 llojet e çrregullimit të informacionit

Në vitin 2017, e krijova tipologjinë vijuese për t'i nënvizuar llojet e ndryshme të çrregullimit të informacionit që ekzistojnë.



Satirë ose Parodi – Nuk ka qëllim për të shkaktuar dëm, por ka aftësi të mashtrojë
Përmbajtje çorientuese – Përdorim keqorientues i përmbajtjes për t'i prezantuar një çështjeje ose individ në mënyrë të dëshiruar
Përmbajtje mashtruese – kur imitohen burimet e vërteta
Përmbajtje e fabrikuar – Përmbajtja e re është 100% e rreme, e krijuar për të mashtruar dhe për të bërë dëm
Lidhje e rreme – kur titujt, vizualizimet ose titrat nuk e përkrahin/nuk përputhen me përmbajtjen
Kontekst i rremë – Kur përmbajtja e vërtetë shpërndahet me informacion të rremë kontekstual
Përmbajtje e manipuluar – kur informacioni ose imazhi autentik manipulohet për të mashtruar

Satirë/Parodi

Është e kuptueshme që shumë njerëz e kanë kundërshtuar futjen time të satirës në këtë tipologji, dhe sigurisht që kam hasur në vështirësi për përfshirjen e kësaj kategorie. Por fatkeqësisht, agjentët e dezinformatave e emërojnë qëllimisht përmbajtjen si satirë për t'u siguruar se nuk do të jetë e nënshtruar verifikimit të fakteve, dhe si mënyrë për gjetje të arsyetimit për ndonjë dëm që mund të vijë nga përmbajtja. Në një ekosistem informativ, ku konteksti dhe sugjerimet, ose shkurtesat mendore (heueristiket) janë zhveshur, përmbajtja satirike ka më shumë gjasë ta vërë lexuesin në konfuzion. Një amerikan mund ta dijë që The Onion është faqe satirike, por a e dini që, sipas Uikipedias, ekzistojnë rreth 57 uebfaqe satirike në botë? Nëse nuk e dini që uebfaqja është satirike e ju shfaqet në feed-in (kronologjinë) e Facebook-ut, është e lehtë të mashtroheni.

Së fundmi, Facebook-u ka marrë vendimin që të mos i verifikojë faktet në satira, por ata që punojnë në këtë hapësirë e dinë se si përdoret emërtimi si satirë për një dredhi e qëllimshme. Në fakt, në gusht të vitit 1919, organizata e që punon në përgënjeshtrimin e përmbajtjeve Snopes shkroi një artikull se pse ata kryejnë verifikim të fakteve në satira. Përmbajtja që pretendon të jetë satirë do t'i shmangë të gjithë verifikuesit e fakteve, dhe shpesh përgjatë kohës, konteksti origjinal do të humbet; njerëzit e shpërndajnë dhe rishpërndajnë duke mos e vënë re që përmbajtja është satirë dhe duke e besuar se është e vërtetë.

Lidhje e rreme

Kjo është modë e vjetër e klik-bejtit (click-bait): teknikë e pretendimeve në lidhje me përmbajtjen përmes titujve sensacionalë, që më pas të kuptohet se titulli nuk ka fare lidhje me artikullin apo përmbajtjen. Derisa është e lehtë për mediat informative të mendojnë se problemi i dezinformatave është i shkaktuar nga aktorët e këqij, unë argumentoj që është e rëndësishme të njohim që praktikat e këqija brenda gazetarisë janë sfidë shtesë e çrregullimit të informacionit.

Përmbajtje çorientuese

Kjo është diçka që ka qenë çdoherë problem në gazetari dhe politikë. Pavarësisht nëse bëhet fjalë për përzgjedhje të një segmenti të pjesshëm nga një citat, krijim të statistikave që përkrahin një pretendim të caktuar por nuk marrin parasysh se si është krijuar grupi i të dhënave, ose prerja (kropimi) i një fotografie për ta interpretuar një ngjarje në mënyrë të caktuar, këto lloje të praktikave çorientuese, sigurisht që nuk janë të reja.

Konteksti i rremë

Kjo është kategori që e hasim në shumicën e përmbajtjeve: gati çdoherë ndodh kur pamjet autentike të vjetra rishpërndahen si të reja. Kjo ndodh shpesh gjatë një ngjarjeje që emërtohet si 'lajm i fundit' (breaking news) kur rishpërndahen imazhe të vjetra, por ndodh gjithashtu kur artikujt e vjetër të lajmeve rishpërndahen si të reja, gjegjësisht kur titulli potencialisht përshtatet ende me ngjarjet bashkëkohore.

Përmbajtje mashtruese

Kjo ndodh kur logoja e një brendi apo emri të njohur përdoret përkrah përmbajtjes së rreme. Kjo taktikë është strategjike sepse bën lojë me rëndësinë e heueristikës. Një nga mënyrat më të fuqishme me të cilat gjykojmë përmbajtjen është nëse është krijuar nga një organizatë apo person të cilit veç më i besojmë. Kështu, duke marrë një logo të një organizate të besueshme të lajmeve dhe duke e vendosur në fotografi apo video, kjo automatikisht e rrit mundësinë që njerëzit ta besojnë përmbajtjen pa e kontrolluar.

Përmbajtje e manipuluar

Kjo ndodh kur përmbajtja origjinale është e ndryshuar apo e modifikuar në ndonjë mënyre. Videoja e Nensi Pelosit në maj të vitit 2019 është një shembull i kësaj. Kryetarja e Dhomës së Përfaqësuesve të SHBA-së është filmuar duke mbajtur një fjalim. Vetëm pak orë më vonë, u shfaq një video e saj duke folur dhe duke e bërë të tingëllonte sikur e dehur. Videoja ishte ngadalësuar dhe duke vepruar kështu, dukej sikur ajo po i belbëzonte fjalët e saj. Kjo është një taktikë e fuqishme, sepse është e bazuar në filmim autentik. Nëse njerëzit e dinë se ajo ka mbajtur fjalimin me atë sfond, kjo i bën që të besojnë më shumë në atë që kanë parë.

Përmbajtje e fabrikuar

Kjo kategori është në rastet kur përmbajtja është 100% e fabrikuar. Kjo mund të jetë krijimi i një llogarie të re tërësisht të rreme në media sociale dhe shpërndarja e përmbajtjes së re nga ajo. Kjo kategori përfshin edhe dip-fejks (deep-fakes ose falsifikime të thella), ku inteligjenca artificiale përdoret për të krijuar video apo audio fajl, në të cilin dikush thotë apo bën diçka që realisht kurrë nuk e ka thënë ose bërë.

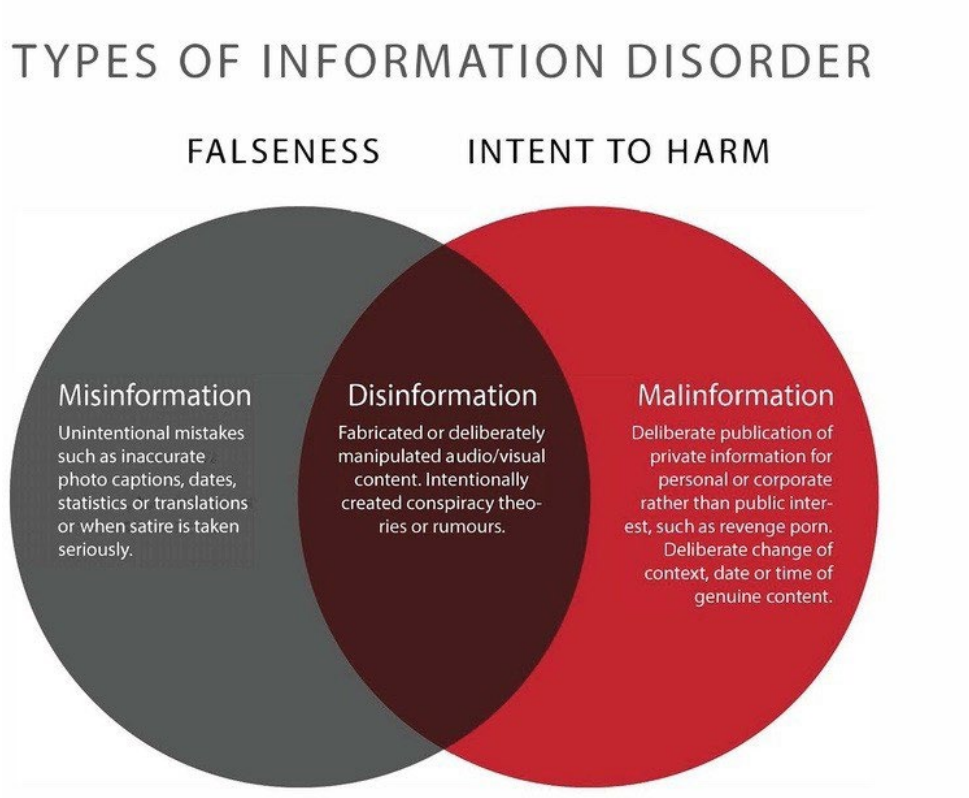
Të kuptuarit e qëllimit dhe motivimit

Kjo tipologji është e dobishme për të shpjeguar kompleksitetin e mjedisit të ndotur të informacionit, por nuk e trajton çështjen e qëllimit. Kjo është një pjesë thelbësore për të kuptuar këtë fenomen.

Për ta bërë këtë, Derakhshan dhe unë hartuam këtë diagram të Venit si një mënyrë për të shpjeguar ndryshimin mes keqinformimit, dezinformimit dhe një term të tretë që krijuam, malinformimit apo informatave malicioze (malinformation). Keqinformimi dhe dezinformimi, të dyja janë shembuj të përmbajtjes së rreme. Mirëpo dezinformata krijohet dhe shpërndahet nga

njerëz që shpresojnë të bëjnë dëm, qoftë dëm financiar, në reputacion, politik apo fizik. Keqinformimi është gjithashtu i rremë, por njerëzit që e shpërndajnë përmbajtjen nuk e kuptojnë se është e rreme. Ky është rast i shpeshtë gjatë ngjarjeve të lajmeve të fundit kur njerëzit ndajnë thashetheme ose fotografi të vjetra duke mos e kuptuar se nuk janë të lidhura me ngjarjet.

Malinformacioni është informacion autentik, mirëpo njerëzit që e shpërndajnë përpiqen të shkaktojnë dëm. Një shembull për këtë është "rrjedhja" (publikimi) i e-mailave të Hillari Klintonit gjatë fushatës presidenciale të vitit 2016. E tillë është edhe shpërndarja e pornografisë hakmarrëse.



LLOJET E ÇRREGULLIMIT TË INFORMACIONIT
FALSITETI / QËLLIMI PËR TË SHKAKTUAR DËM

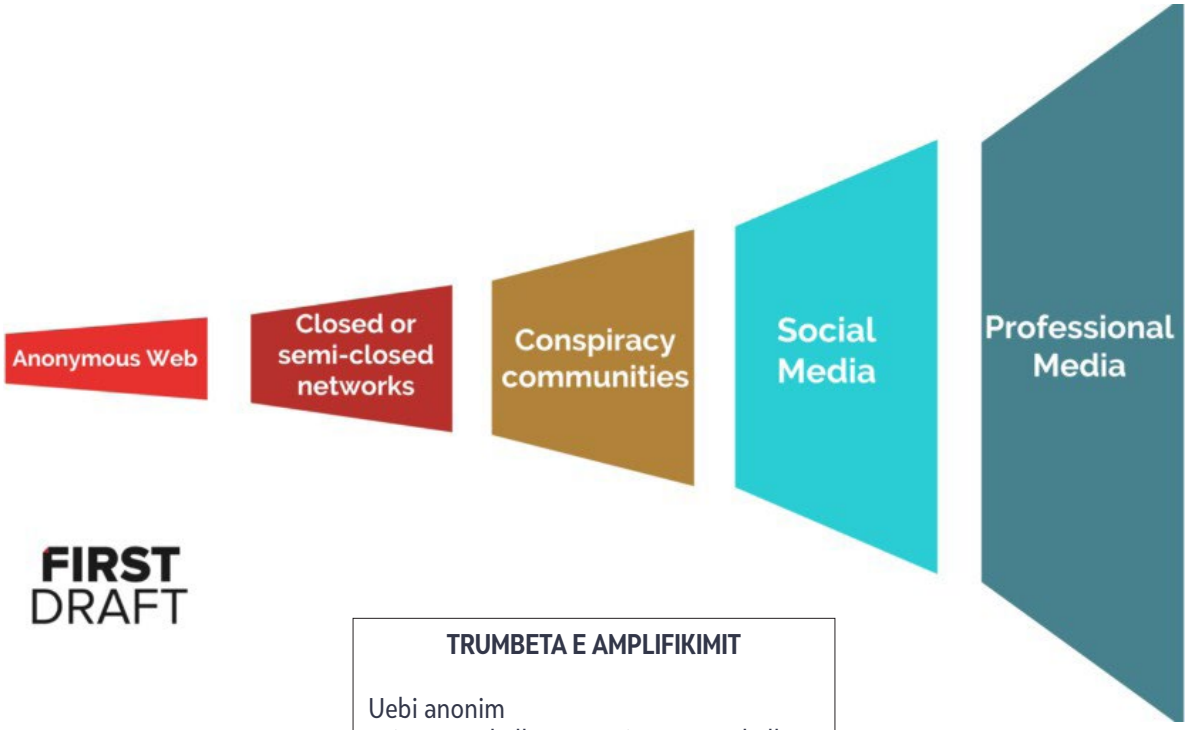
Informata të gabuara (misinformata) – Gabime të paqëllimshme, siç janë tekstet e gabuara nën foto, datat, statistikat ose përkthimet, ose kur satira merret për seriozisht.
Dezinformata – Përmbajtje audio/vizuale e fabrikuar ose e manipuluar qëllimisht. Thashetheme ose teori të konspiracionit të krijuara me qëllim.
Malinformata (informata malicioze) – Publikim i qëllimshëm i informatave private të një personi ose korporate përkundër interesit publik, si pornografi hakmarrëse. Ndryshim i qëllimshëm i kontekstit datës ose kohës së kontekstit autentik.

Këto terme kanë rëndësi, sepse qëllimi është pjesë e asaj si duhet ta kuptojmë një informacion të caktuar. Ekzistojnë tre lloje kryesore të motivimit për krijimin e përmbajtjes të rreme dhe çorientuese. I pari është politik, qoftë politikë e jashtme apo e brendshme. Mund të jetë rast i ndonjë qeverie të huaj që përpiqet të ndërhyjë në zgjedhjet e ndonjë shteti tjetër. Mund të jetë rast i brendshëm, ku një fushatë angazhohet në taktika "të fëlliqura" (dirty) për ta njollosur kundërshtarin. I dyti është financiar. Është e mundur të bësh para nga reklamimi në faqen tënde. Nëse ke artikull sensacional të rremë me titull hiperbolik, përderisa mund t'i bësh njerëzit të klikojnë URL-në tënde, mund të bësh para. Njerëzit nga të dy anët e spektrit politik kanë folur për atë se si kanë krijuar dhe fabrikuar faqe "të lajmeve" për të përfituar klikime, e kështu edhe të ardhura. Në fund, janë faktorët shoqëror dhe psikologjik. Disa njerëz janë të motivuar thjeshtë nga dëshira për të shkaktuar telashe dhe për të parë se çfarë mund të përfitojnë me këtë; të shohin se a mund t'i mashtrojnë gazetarët, të krijojnë ngjarje në Facebook që i shtyjnë njerëzit të dalin jashtë në rrugë për të protestuar, për të bullizuar dhe ngacmuar gratë. Të tjerët përfundojnë duke e shpërndarë keqinformimin, pa arsye tjetër pos dëshirës së tyre për të përfaqësuar një identitet të caktuar. Për shembull, dikush që thotë, "nuk më intereson nëse nuk është e vërtetë, unë vetëm dua t'ua theksoj shokëve të mi në Facebook se sa e urrej [vendos emrin e kandidatit.

Trumbeta e amplifikimit

Për ta kuptuar vërtetë këtë ekosistem më të gjerë, duhet ta shohim se si ndërlidhen të gjitha këto gjëra. Shumë shpesh, dikush e sheh diku një përmbajtje keqorientuese ose të rreme, dhe beson se është krijuar atje. Fatkeqësisht, ata që janë më efektivë kur flitet për dezinformim e kuptojnë se si ta shfrytëzojnë natyrën e tij fragmentuese.

Po ashtu duhet mbajtur mend se, në qoftë se thashethemet, konspiracionet, apo përmbajtjet e rreme nuk do të shpërndaheshin, nuk do të kishin shkaktuar dëm. Është shpërndarja ajo që është me të vërtetë dëmtuese. Prandaj e krijova këtë imazh, që e quaj Trumbeta e Amplifikimit, si mënyrë për të përshkruar se si agjentët e dezinformatave e përdorin koordinimin për ta lëvizur informacionin nëpër këtë ekosistem.



Shpeshherë, përmbajtja publikohet në hapësira si 4Chan ose Discord (aplikacion i përdorur nga gejmerët/lojtarët e video lojërave për të komunikuar). Këto hapësira janë anonime dhe lejojnë njerëzit të postojnë pa adresë. Shpesh këto hapësira përdoren për të shpërndarë detaje specifike mbi koordinimin, si "do të provojmë ta bëjmë këtë hashtag të jetë në trend", ose "përdoreni këtë meme për t'iu përgjigjur ngjarjeve të sotme në Facebook".

Më pas, koordinimi shpesh bartet në grupe më të mëdha për mesazhe direkte (DM) të Twitterit apo grupe në WhatsApp (Uatsapit) ku nyjat (nodes) përbrenda rrjetit shpërndajnë përmbajtje te një grup më i gjerë i njerëzve. Pastaj mund edhe të bartet në komunitete në faqe tjera si Gab, Reddit ose në YouTube. Nga atje, përmbajtja shpeshherë shpërndahet në faqe më me ndikim (mainstream), si Facebooku, Instagrami, apo Twitteri.

Nga atje, shpeshherë ndodh që përmbajtja të merret edhe nga mediat profesionale - ose sepse nuk e kuptojnë prejardhjen e përmbajtjes dhe vendosin ta përdorin në raportimin e tyre pa verifikim të mjaftueshëm, ose sepse vendosin ta përgënjeshtrojnë përmbajtjen. Sidoqoftë, agjentët e dezinformimit e shohin këtë si një sukses. Titujt e mangët ku raportohen thashethemet apo pretendimet çorientuese, ose përgënjeshtrimet ku përmbajtja e rreme është e përfshirë (e embeduar) në tregim, i shkojnë për shtati planit origjinal: për të nxitur amplifikimin, gjegjësisht për t'u dhënë frymë thashethemeve.

Në First Draft, ne flasim për konceptin e pikës së kthesës. Për gazetarët, raportimi tejet i hershëm mbi gënjeshtrat ofron frymë shtesë dhe potencialisht të dëmshme për thashethemet. Raportimi tejet i vonshëm do të thotë se ato kanë zënë vend dhe se lidhur me to mund të bëhet shumë pak. Gjetja e kësaj pike kthese është sfiduese. Ajo ndryshon sipas vendndodhjes, temës dhe platformës.

Përfundim

Gjuha ka rëndësi. Ky fenomen është kompleks dhe fjalët që i përdorim e bëjnë dallimin. Veç më kemi hulumtime akademike që tregojnë se te audiencat është vazhdimisht në rritje e barazojnë përshkrimin "lajme të rreme" (fake news) me praktika të raportimit të dobët nga mediat profesionale.

Përshkrimi i gjithçkaje si dezinformatë, kur realisht mund të mos jetë përmbajtje e rreme, ose kur shpërndahet nga njerëzit pa e ditur që është e rreme, janë elemente tjera kyçe për të kuptuar se çfarë po ndodh.

Jetojmë në një epokë të çrregullimit të informacionit. Ai po krijon sfida të reja për gazetarët, hulumtuesit dhe profesionistët e informacionit. Të raportosh apo të mos raportosh? Çfarë fjalësh të përdoren në titujt? Si të përgënjeshtrohen videot dhe fotografitë në mënyrë efektive? Si të dish kur t'i verifikosh? Si mund të matet një pikë kthese? Të gjitha këto janë sfida të reja që ekzistojnë sot për ata që punojnë në mjedisin e informacionit. Është një gjë e komplikuar.

Cikli jetësor i manipulimit mediatik

Shkruan: Xhoan Donovan

Dr. Xhoan Donovan *(Joan Donovan) është drejtoreshë e hulumtimit në Qendrën Shorenstein të Kenedit për Media, Politikë dhe Politika Publike në Universitetin e Harvardit.*

Në një epokë ku një grusht i platformave të fuqishme globale kanë çrregulluar mjetet tradicionale me të cilat informohet shoqëria, manipulimet mediatike dhe fushatat e dezinformatave sot sfidojnë të gjitha institucionet politike dhe shoqërore. Mashtrimet dhe fabrikimet propagandohen nga një grup i përzier e operativëve politik, brendeve (markave), lëvizjeve shoqërore dhe "trollëve" pa përkatësi që kanë zhvilluar dhe rafinuar teknika të reja për të ndikuar në diskutimet publike, duke bërë kërdi në nivel lokal, nacional dhe global. Ekziston një pajtim i gjerë se manipulimet mediatike dhe dezinformatat janë probleme të rëndësishme me të cilat po përballet shoqëria. Mirëpo, definimi, detektimi, dokumentimi, dhe zbulimi i dezinformatave dhe manipulimeve mediatike mbetet i vështirë, veçanërisht pasi sulmet kalojnë në sektorët profesional si gazetaria, drejtësia dhe teknologjia. Prandaj, të kuptuarit e manipulimit mediatik si një aktivitet i modeluar është hapi i parë thelbësor në punën për hetimin, ekspozimin dhe menaxhimin e tyre.

Definimi i manipulimeve mediatike dhe dezinformatave

Për ta definuar manipulimin mediatik, së pari duhet ta ndajmë termin në dy pjesë. Në formën e saj më të përgjithshme, media është një artefakt i komunikimit. Shembujt përfshijnë tekstin, fotografitë, audio, dhe video në material dhe në media digjitale. Gjatë studimit të medias, çdo relikt mund të përdoret si provë e regjistruar e një ngjarjeje. Thelbësore është ajo se media është e krijuar nga individët me qëllim të komunikimit. Në këtë mënyrë, media përcjell njëfarë kuptimi te individët, por interpretimi i atij kuptimi është çdoherë relacional dhe i vendosur përbrenda një konteksti të distribuimit.

Të pretendosh se media është e manipuluar do të thotë të shkosh përtej pohimit të thjeshtë se media është krijuar nga individë për të përçuar një kuptim me qëllim. Fjalori Merriam-Webster e definon manipulimin si "të ndryshosh me mjete të shkathëta dhe të padrejta për t'i shërbyer qëllimit të dikujt". Përderisa ndonjëherë mund të jetë e vështirë të dihet qëllimi i saktë për të cilin shërben një artefakt i krijuar, hulumtuesit mund të përcaktojnë pyetjet "kush", "çfarë", "ku" dhe "si" të komunikimit për të ndihmuar në përcaktimin nëse taktikat manipuluese janë përdorur si pjesë e procesit të distribuimit. Taktikat e manipulimit mund të përfshijnë fshehjen e identitetit të dikujt ose të burimit të artefaktit, redaktimin (montazhin) për ta fshehur apo ndryshuar kuptimin ose kontekstin e një artefakti, si dhe mashtrimin e algoritmeve përmes përdorimit të koordinimit artificial, siç është përdorimi i bot-ëve dhe mjeteve për spamming (reklamim mashtrues).

Në këtë kontekst, dezinformimi është një nën-zhanër i manipulimit mediatik, dhe i referohet krijimit dhe shpërndarjes së qëllimshme të informacioneve të rreme për qëllime politike. Teknologët, ekspertët, shkencëtarët, gazetarët dhe politikbërësit patjetër duhet të pajtohen për kategorinë dalluese të dezinformimit, sepse përpjekjet për të luftuar kundër dezinformatave kërkojnë bashkëpunimin e këtyre grupeve.

Nga ana jonë, ekipi kërkimor i Teknologjisë dhe Ndryshimeve Sociale (TaSC) në Qendrën Shorenstein të Shkollës Kennedy të Harvardit po përdor një qasje të rasteve të studimit për të hartuar ciklin jetësor të fushatave të manipulimit të medias. Kjo qasje metodologjike tenton të analizojë rendin, shkallën dhe shtrirjen e fushatave të manipulimit duke ndjekur artefaktet mediatike nëpër hapësirë dhe kohë, duke tërhequr së bashku marrëdhënie të shumta për të zgjidhur rrëmujën e koklavitur. Si pjesë e kësaj pune, kemi zhvilluar një përmbledhje të ciklit jetësor të një fushate të manipulimit mediatik, e cila është e dobishme për gazetarët gjatë përpjekjeve që të identifikojnë, gjurmojnë dhe ekspozojnë manipulimet mediatike dhe dezinformatat.

Cikli jetësor i një fushate për manipulim mediatik

1. Planifikimi i fushatës manipuluese
2. Mbjellja apo shpërndarja e fushatës nëpër platforma sociale dhe ueb
3. Reagimet nga industria, aktivistët, politikanët dhe gazetarët
4. Ndryshimet në ekosistemin mediatik
5. Përshtatjet nga manipuluesit ndaj mjedisit të ri

Cikli jetësor ka pesë pika veprimi, ku taktikat e manipuluesve mediatikë mund të dokumentohen duke përdorur metoda kualitative dhe kuantitative. Vini re se shumica e fushatave të manipulimit nuk "zbulohen" në këtë renditje. Në vend të kësaj, kur hulumtoni, kërkoni ndonjë nga këto pika veprimi dhe më pas gjurmoni fushatën prapa dhe përpara përgjatë ciklit jetësor.

Rasti studimi: *'Blow the Whistle' ("Fryji bilbilit" – ose denonco)*

Të shqyrtojmë aktivitetin e mediave sociale rreth ankesës së një denoncuesi (whistleblower) të bërë në lidhje me aktivitetin e presidentit Donald Tramp lidhur me Ukrainën, për të parë se si shpaloset fushata e manipulimit mediatik, dhe se si veprimi i hershëm etik i gazetarëve dhe platformave gjatë ciklit jetësor mund të ndihmojë në pengimin e përpjekjeve të manipulimit.

Planifikimi dhe mbjellja (Fazat 1 dhe 2) - Në ekosistemin mediatik të teorisë së konspiracionit, identiteti i denoncuesit është tashmë i njohur dhe emri i tij po qarkullon në bllogje, Twitter, Facebook, video në YouTube dhe forume diskutimi. E rëndësishmja është që emrat unik mund të zëvendësojnë fjalë kyçe dhe hashtagje, të cilat funksionojnë si pika diskrete të të dhënave të kërkueshme. Pati një shtytje të përbashkët për të përhapur emrin e supozuar dhe fotografinë e personit. Megjithatë, emri duket se është i mbyllur në këtë jehonë mediatike onlajn të llogarive dhe entiteteve të krahut të djathtë dhe konspirativ. Edhe krahas kësaj përpjekjeje të koordinuar nga influencuesit konspiracionistë për të shtyrë emrin e denoncuesit në mejnstrim, ata nuk ishin në gjendje të dilnin nga filtrat e "flluskave" (bubbles) ku veprojnë. Pse ndodh kjo?

Përgjigjet e gazetarëve, aktivistëve etj. (Faza 3) — Në kontrast me këtë, mediat e majta dhe ato centriste nuk e publikuan emrin e denoncuesit të supozuar ose nuk i amplifikuan pretendimet se ai ishte zbuluar. Mediat me ndikim të madh (mainstream) u përmbajtën nga dhënia e vëmendjes ndaj qarkullimit të emrit të këtij personi në ekosistemin e mediave sociale, edhe pse kjo është një tregim i përshtatshëm për lajme për gazetarët e teknologjisë dhe politikës. Ata që e mbuluan këtë lajm theksuan shpesh se si akti i qarkullimit të këtij emri ishte një përpjekje për të manipuluar diskutimin rreth ankesës së denoncuesit dhe iu shmangën përhapjes së emrit të tij. Kjo është kryesisht për shkak të etikës së gazetarisë, ku reporterët kanë detyrë të veçantë për të mbrojtur anonimitetin e burimeve, që shtrihet edhe për denoncuesit.

Ndryshimet në ekosistemin e informacionit (Faza 4) - Përderisa mejnstrim gazetarët i shmangeshin botimit të emrit të tij, emri i supozuar i denoncuesit, "Eric Ciaramella", është një fjalë kyçe unike. Kjo do të thoshte se njerëzit që e kërkuan atë mund të nxirrnin një larmi të gjerë përmbajtjesh të rrënjosura në këndvështrimin e ndikuar nga konspiracionet. Përveç gazetarëve etikë që refuzuan në mënyrë efektive një storie që mund të tërhiqte trafik të konsiderueshëm, secila kompani e platformave filloi të moderonte në mënyrë aktive përmbajtjen që përdorte emrin e denoncuesit të supozuar si fjalë kyçe. YouTube dhe Facebooku i hiqnin përmbajtjet që përdornin emrin e tij, ndërsa Twitter pengoi që emri i tij të bëhej trend. Kërkimi në Google lejoi që emri i tij të jetë i kërkueshëm dhe kthente mijëra lidhje që çonin në bllogje të teorive konspirative.

Përshtatjet nga manipuluesit (Faza 5) — Manipuluesit u irrituan nga këto përpjekje për të parandaluar përhapjen e informatave të gabuara (misinformacione) dhe ndryshuan taktikën e tyre. Në vend se të përhapnin përmbajtje me emrin e denoncuesit të supozuar, manipuluesit filluan të qarkullonin imazhe të një njeriu tjetër të bardhë (me syze dhe mjekër) që i përngjante imazhit që e kishin qarkulluar më parë me emrin e tij. Këto imazhe të reja u shoqëruan me një narrativë teorish konspiracioni për "shtetin e thellë" (deep state), duke pretenduar se informatori ishte mik i establishmentit të Demokratëve, dhe prandaj ka pasur motive partiake. Megjithatë, ky ishte një imazh i Aleksandër Sorosit, të birit të investitorit dhe filantropit miliarder Xhorxh Soros, i cili është cak i shpeshtë i konspiracioneve.

Kur kjo dështoi të shkaktojë vëmendje mediatike, llogaria e Presidentit Tramp në Twitter @RealDonaldTrump, rituitoi një artikull që jepte emrin e denoncuesit të supozuar, duke u theksuar 68 milionë ndjekësve të tij se "denoncuesi i CIA-s nuk është një denoncues i vërtetë!". Tuiti origjinal erdhi nga llogaria @TrumpWarRoom, e cila është llogari zyrtare dhe e verifikuar e fushatës së tij. Pasoi një përshkallëzim e mbulimit mediatik, duke përfshirë shumë shpërndarës me ndikim, e që të gjithë patën vështirësi për të hequr ose mbuluar emrin e denoncuesit të supozuar. Shumë njerëz bënë thirrje në media sociale që denoncuesi të dëshmojë në dëgjimet për impiçment (shkarkim të presidentit) në Senat, ku emri i tij u përmend së bashku me dëshmitarë të tjerë potencialë të rëndësishëm, duke zgjeruar kështu mundësinë që të tjerë të hasin në këtë emër kur kërkojnë emra të tjerë. Dhe, kështu fillon një cikël i ri i manipulimeve mediatike.

Kërkesat për emrin e denoncuesit janë në rritje, e bien në sy edhe teoritë konspirative në bllogje rreth motiveve personale dhe profesionale të tij për të njoftuar mbi aktivitetet e Trampit. Gazetarët që raportojnë për këto tuite lëkunden midis diskutimeve mbi frikësimin e dëshmitarëve, duke cituar se një akt i tillë mund të ndikojë në parandalimin e denoncuesve të ardhshëm, ndërsa po ashtu bien në kuriozitetin sensacional duke raportuar mbi thashethemet rreth motivimit të Trampit për zbulimin e denoncuesit. Si e tillë, është për lëvdatë që disa organizata mediatike përpiqen t'u kërkojnë llogaridhënie elitave, por kjo detyrë është e pamundur nëse kompanitë e platformave nuk e adresojnë mënyrën se si produktet e tyre janë bërë mjete politike efikase për manipulime mediatike dhe përhapje të dezinformatave.

Dokumentimi i ciklit jetësor

Manipuluesit e medias u përpoqën të "tregtojnë zinxhirin" duke mbjellë një emër dhe fotografi në mediat sociale, në mënyrë që të shkaktojnë eventualisht që mediat e mëdha dhe legjitime ta amplifikojnë atë, ku platformat do ta lejonin atë të bëhej trend dhe të bëhet përmbajtje lehtësisht e zbulueshme. Por vendimet dhe veprimet e platformave dhe gazetarëve bënë që përpjekja për të shtyrë identitetin e pretenduar të denoncuesit në vetëdijen e përgjithshme (mainstream) kryesisht të dështonte, deri sa një figurë e rëndësishme e lajmeve e shtyu çështjen. Përderisa shumë organizata mediatike përpiqen të ndjekin udhëzimet etike, mediat sociale janë bërë armë e atyre që veçmë janë të fuqishëm për të kurdisur agjendat e mediave dhe për t'u dhënë shtytje teorive të rrezikshme të konspiracionit.

Megjithatë, në përgjithësi, ky rast studimi është një përmirësim domethënës në krahasim me përpjekjet e mëparshme për të ndaluar përhapjen e dezinformatave, ku gazetarët amplifikuan fushatat e dezinformimit përderisa përpiqeshin t'i përgënjeshtronin, kurse kompanitë e platformave nuk ndjenin asnjë detyrim për të ofruar informacion të saktë për audiencën. Ky ndryshim i përgjithshëm është premtues, por përgjegjësia për elitat ende mungon. Për gazetarët dhe studiuesit e ngjashëm, rreziku i zbulimit, dokumentimit dhe përgënjeshtrimit të fushatave të manipulimit të medias është i lartë. Në këtë moment hiper-partiak, çdo pretendim për të emërtuar një fushatë dezinformimi mund të sjellë gjithashtu një mori trollësh dhe vëmendje të padëshiruar. Ballafaqimi me përmbajtjen dhe kontekstin e dezinformatave kërkon nga të gjithë ne dokumentim forenzik dhe rigoroz të mënyrës se si fushatat fillojnë, ndryshojnë dhe përfundojnë. Si dhe për të njohur se çdo fund i perceptuar i një fushate mund të jetë po aq një fillim i ri.

1. Hetimi i llogarive të mediave sociale

Shkruan: Brendi Zadrozni

Brendi Zadrozni *(Brandy Zadrozny) është reportere hulumtuese për NBC News, ku më së shumti mbulon informatat e gabuara (misinformatat), dezinformatat dhe ekstremizmin në internet*

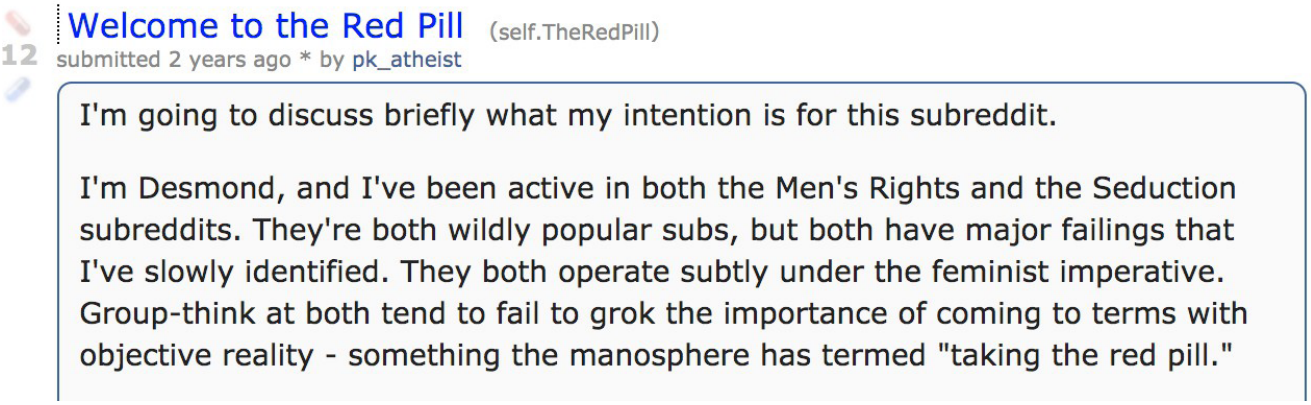
Pothuajse çdo storie që raportoj përfshin hulumtimin e mediave sociale. Nga kërkimi i bekgraundit (prapavijës) së profilit te lajmet e fundit e deri te hulumtimet më të gjata, platformat e mediave sociale ofrojnë disa nga mënyrat më të mira për të mësuar rreth jetës reale të një subjekti – familjes, miqve, marrëdhënieve të punës, politikave personale dhe lidhjeve – si dhe një dritare në mendimet e fshehta dhe identitetet e fshehura onlajn.

Është një kohë e mahnitshme për të qenë gazetar; njerëzit e jetojnë gjithnjë e më shumë jetën e tyre në internet, e mjetet për të gjetur dhe kërkuar profilet sociale të një subjekti gjenden kudo. Në të njëjtën kohë, si njerëzit e zakonshëm ashtu edhe aktorët e këqij po bëhen më të zgjuar në fshehjen e gjurmëve të tyre. Ndërkohë, platformat e mediave sociale si Facebook kanë reaguar ndaj mbulimit negativ mediatik në lidhje me shkeljet e privatësisë dhe ideologjitë e dëmshme të përhapura në platformën e tyre duke mbyllur mjetet në të cilat janë mbështetur gazetarët dhe studiuesit për të zbuluar storiet dhe për të identifikuar njerëzit.

Në kapitullin vijues do të tregoj disa qasje thelbësore për hetimin e llogarive sociale. Mjetet janë ato që i përdor aktualisht, por pa kaluar shumë kohë ato do të vriten nga Facebooku ose do të zëvendësohen nga diçka më e mirë. Gazetarët që janë më të mirët në këtë punë kanë proceset dhe pajisjet e tyre personale për të arritur te caku, por në të vërtetë, si te çdo brend i raportimit, obsesioni dhe lëkura (virtuale) e këpucëve japin rezultatet më të mira. Përgatituni për të lexuar mijëra tuit, klikoni deri në fund të rezultateve në Google dhe zhytuni deri në fund të "vrimës së lepurit" në mediat sociale nëse dëshironi të grumbulloni gjurmë të vogla biografike që do t'ju ndihmojnë t'i përgjigjeni pyetjes: "Kush është ky/kjo?"

Emrat e përdoruesve (Usernames)

Një emër përdoruesi është ndonjëherë gjithçka që kemi, gjë që është në rregull, sepse është pothuajse gjithmonë pika ku fillojmë. I tillë ishte rasti i një republikani përfaqësues i atëhershëm i shtetit në Nju Hempshir, i cili ndërtoi një nga komunitetet më të njohura dhe më të urryera të meshkujve në Reddit. Hetimi pas demaskimit të arkitektit të komunitetit Pilula e Kuqe (The Red Pill) në Reddit, tani një komunitet i karantinuar, filloi me emrin e përdoruesit "pk_atheist".



Disa njerëz mbajnë emrat e përdoruesve, duke i përdorur ato me variacione minimale nëpër platforma të ndryshme dhe provajderë të postës elektronike (e-mailave). Ata që janë më të fokusuar në siguri, si përfaqësuesi i shtetit të Nju Hempshir, krijojnë dhe hedhin emrat e përdoruesve me çdo përpjekje të re.

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

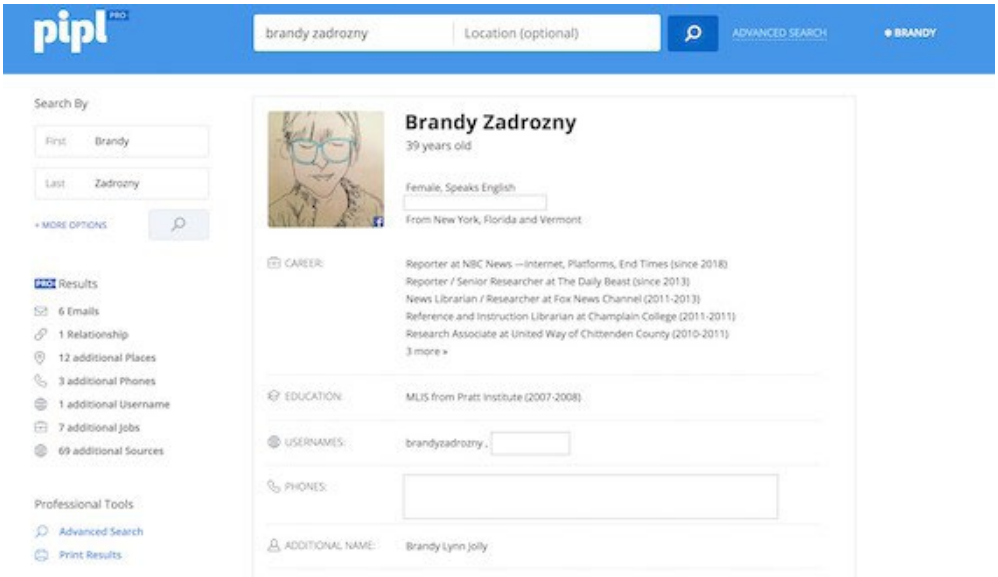
I don't think we can grow if we ever go private. It goes without saying, you should invest in a decent throwaway that cannot be traced back to you.

permalink **embed** **parent**

Sido që të jetë rasti, ka disa sajte në të cilat duhet të futni emrin e përdoruesit që po kërkoni.

Së pari, e fus emrin e përdoruesit në Google. Njerëzit - veçanërisht ata më të rinjtë që u shmangen platformave më të mëdha sociale - priren të lënë gjurmë edhe në vende nga më të papriturat, duke përfshirë seksionet e komenteve, rishikimet dhe forumet, gjë që mund t'ju drejtojë në informacione dhe llogari të tjera.

Së bashku me kërkuesin e Google, përdorni shërbimet për të dhënat pronësore. Ato kushtojnë para dhe në varësi nga buxheti i redaksisë suaj, mund të keni apo të mos keni qasje. Shumica e shitoreve kanë Nexis, i cili është i shkëlqyeshëm për të dhëna publike dhe dokumente gjyqësore, por fatkeqësisht ka mangësi në pjesën e e-mailit/emrit të përdoruesit. Gjithashtu, është i dobishëm për të hulumtuar njerëz vetëm në Shtetet e Bashkuara. Pipl dhe Skopenow janë ndër mjetet më të mira që kam gjetur për referencë të kryqëzuar të informacionit të "botës reale" si numrat e telefonit dhe të dhënat e pronave me regjistrimet në internet si e-mailet dhe emrat e përdoruesve, dhe të dyja funksionojnë globalisht. Këta motorë kërkimi me pagesë shpesh ofrojnë të dhëna telefonike dhe të pronësisë, por ata gjithashtu mund të identifikojnë profilet e Facebookut dhe LinkedIn-it që mbeten edhe pasi llogaria të jetë e mbyllur. Ata gjithashtu lidhin llogaritë që njerëzit i kanë harruar në përgjithësi, si bllogjet e vjetra, e madje edhe listat e dëshirave në Amazon - një minierë ari për të mësuar se çfarë lexon, blen dhe dëshiron një person. Me këto gjithashtu mund të merrni edhe shumë të dhëna pozitive por false, kështu që tentoj të filloj hetimin tim me rezultatet e tyre dhe të vazhdoj me mjete të tjera të verifikimit.



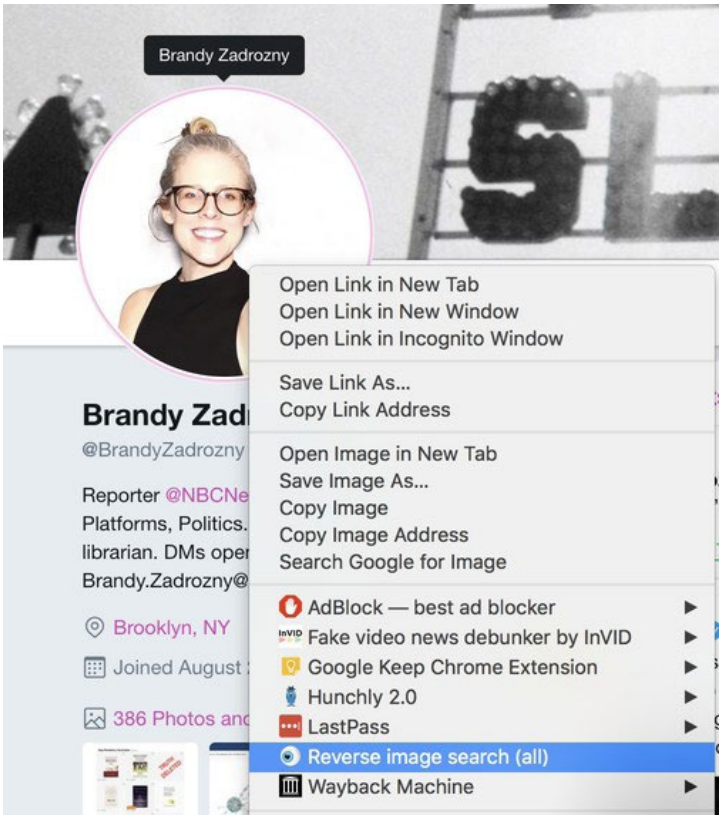
Kur gjej një emër përdoruesi ose e-mail që mendoj se mund t'i përkasë subjektit tim, e fus atë në një mjet onlajn si "namechk" ose "namecheckr" që kërkon disponueshmërinë e emrit të përdoruesit nëpër platforma të ndryshme. Këto mjete janë krijuar për të qenë një mënyrë e lehtë për tregtarët për të parë nëse një emër përdoruesi i caktuar që ata planifikojnë ta regjistrojnë është i disponueshëm nëpër platforma. Por ato janë gjithashtu të dobishme për të kontrolluar nëse një emër përdoruesi që po hetoni ekziston edhe diku tjetër. Natyrisht, vetëm për shkak se një emër përdoruesi është regjistruar në platforma të shumta nuk do të thotë që këto llogari i përkasin të njëjtit person. Por, është një pikënisje e shkëlqyer për të gjurmuar nëpër platforma.

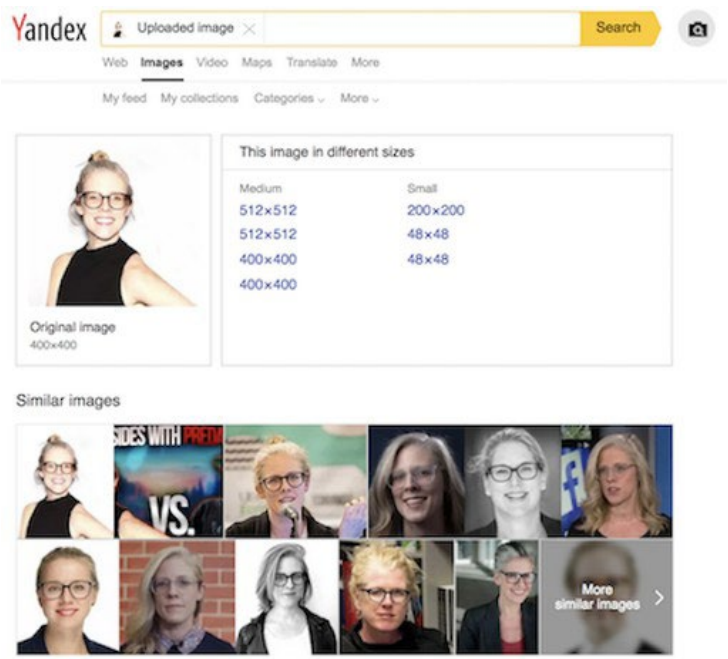
Për kontroll të mëtejshëm të emrit të përdoruesit, ekzistojnë haveibeenpwned.com dhe Dehashed.com, të cilat kërkojnë të dhënat për shkelje të informacionit të përdoruesit dhe mund të jenë një mënyrë e shpejtë për të vërtetuar një adresë e-maili dhe për të siguruar indicie të reja.

Fotografitë

Një emër përdoruesi nuk mjafton gjithmonë për të vazhduar, e asgjë nuk është bindëse si një fotografi. Fotot e profilit janë një mënyrë tjetër për të verifikuar identitetin e një personi nëpër llogari të ndryshme.

Kërkimi i kundërt i imazheve (reversë image search) i Google është i mirë, por shpeshherë janë motorë të tjerë të kërkimit - veçanërisht Yandex i Rusisë – që mund të japin rezultate më të mira. Unë përdor ekstensionin Reveye Chrome Extension, i cili më lejon me klikim të djathtë mbi një imazh të kërkoj përputhjen e tij nëpër platforma të shumta, duke përfshirë Google, Bing, Yandex dhe Tineye. Ekstensioni "Kërkimi sipas imazhit" (Search by Image extension) ka gjithashtu një funksion të shkëlqyeshëm të kapjes që ju lejon të kërkoni nga një imazh brenda një imazhi tjetër.

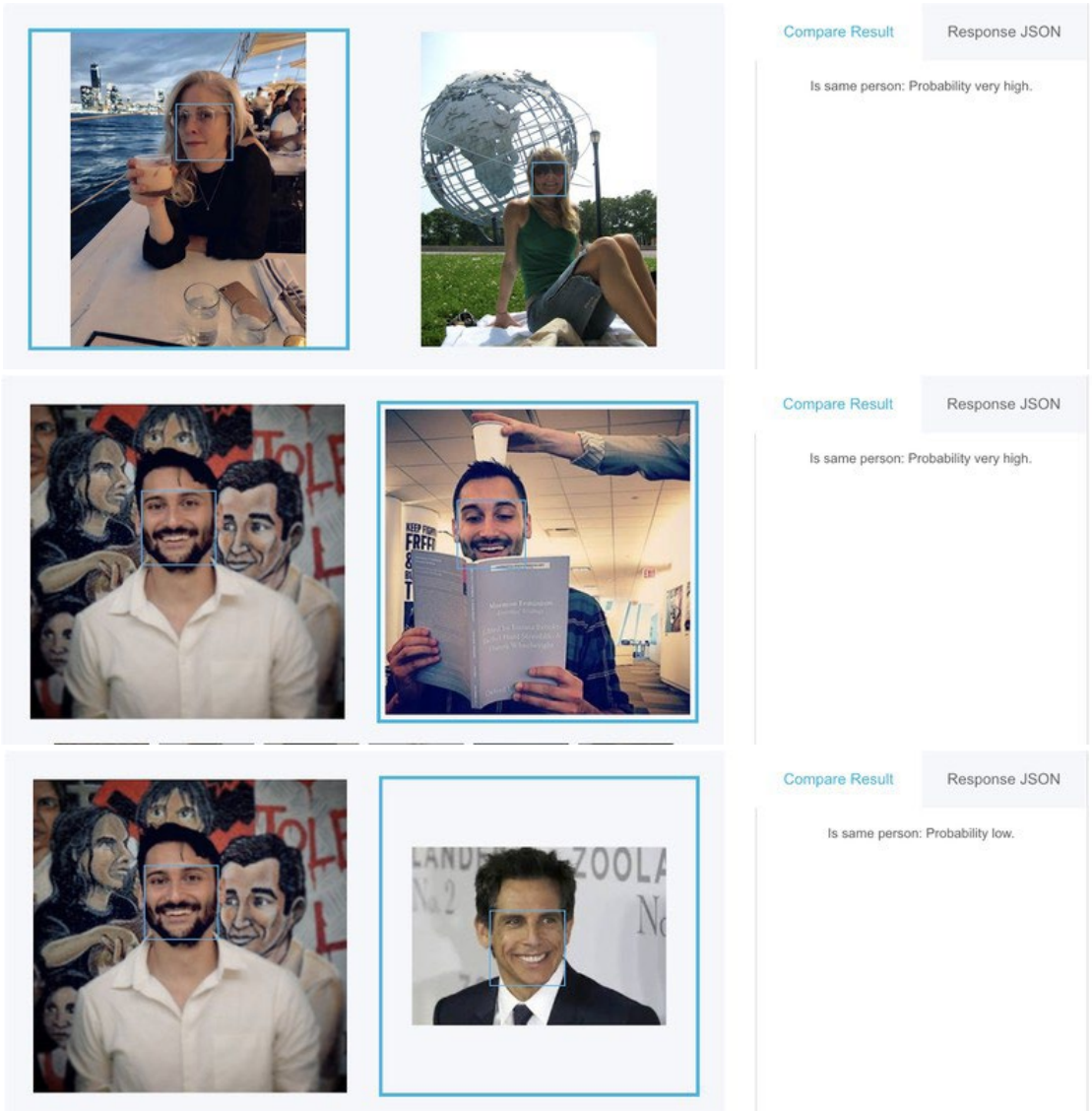




Sigurisht që ka probleme me kërkimin e kundërt të imazhit. Motorët e lartpërmendur të kërkimit bëjnë punë të dobët në gjetjen e imazheve në Twitter dhe janë të padobishëm për nxjerrjen e rezultateve nga faqet si Instagrami dhe Facebooku.

Ajo që kërkoj më shpesh janë imazhe të ndryshme të njerëzve. Nuk mund të numëroj se sa herë e kam vështruar monitorin dhe i kam pyetur kolegët e mi: "A është i njëjti person?"

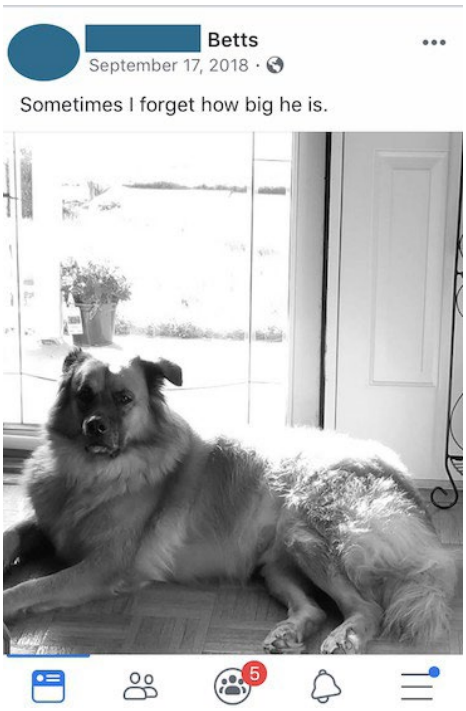
Thjesht, nuk u besoj syve të mi. Identifikimi i karakteristikave nëpër foto si nishanet ose qimet ose tiparet e fytyrës ndihmon; kohët e fundit, po ashtu më pëlqen ta kontrolloj edhe me një mjet për njohjen e fytyrës si Face++, i cili ju lejon të ngarkoni dy foto dhe më pas jep një probabilitet vallë ato i përkasin të njëjtit person. Në këta shembuj, mjeti ishte në gjendje të më identifikonte pozitivisht mua në foto me 10 vite diferencë. Ai gjithashtu identifikoi kolegun tim Benin nëpër fotot e profilit të mediave sociale në Twitter dhe Facebook, ndërsa saktësisht vuri në dukje se ai nuk është, në fakt, Ben Stilleri.

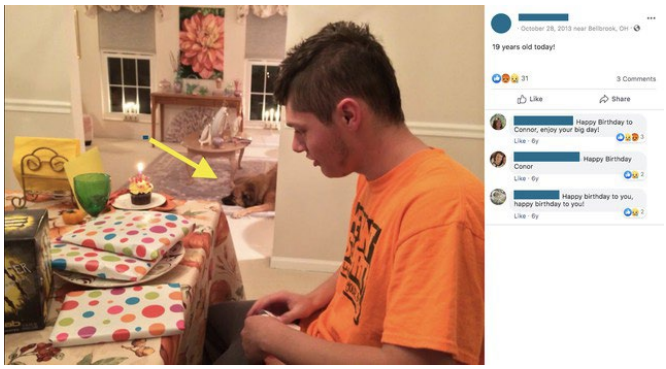


Nëse jeni duke ndjekur trollët ose mashtruesit (scammers), mund të zbuloni se ata kanë bërë më shumë përpjekje për të fshehur fotot e profilit të tyre, ose mund të përdorin foto të rreme. Atëherë editimi i fotografisë dhe rrokullisja e saj mund të ndihmojë në prapakthimin e inxhinjeruar të procesit të tyre.

Megjithatë, nuk janë vetëm fotot e profilit që mund të jenë udhërrëfyes. Gjersa njerëzit bëhen më të vetëdijshëm dhe më të brengosur për privatësinë e tyre dhe të familjes së tyre, ata janë ende të prirë të shpërndajnë foto të gjërave për të cilat krenohen. Kam identifikuar njerëz duke i lidhur me foto të gjërave si makina, shtëpi apo kafshë shtëpiake. Në këtë kuptim, fotografitë bëhen një mjet për të lidhur llogaritë dhe njerëzit që qëndrojnë pas tyre, duke ju mundësuar të ndërtoni rrjetin që ekziston rreth cakut tuaj. Kjo është një praktikë thelbësore kur hetohen llogaritë e mediave sociale.

Për shembull, po kërkonim të konfirmojmë llogaritë sociale të një njeriu që gjuajti dhe vrau nëntë persona jashtë një bari në Dejton, Ohajo. Llogaria e tij në Twitter ofroi gjurmë për ideologjinë e tij politike, por doreza (handle) e tij, @iamthespookster, ishte unike dhe nuk i ngjante emrit të tij të vërtetë, i cili ishte publikuar nga autoritetet. Fakti që një nga viktimat e tij ishte vëllai i tij, një burrë trans-gjinor, emri i të cilit nuk ishte në të dhënat publike dhe nuk kishte dalë ende botërisht, e ndërlikoi më tej identifikimin e figurave kryesore. Por, në të gjithë profilet e tij dhe të familjes së tij kishte foto të një qeni, një kafshe shtëpiake që shfaqej si imazh i banerit të llogarisë së pa raportuar të vëllait të tij trans-gjinor.



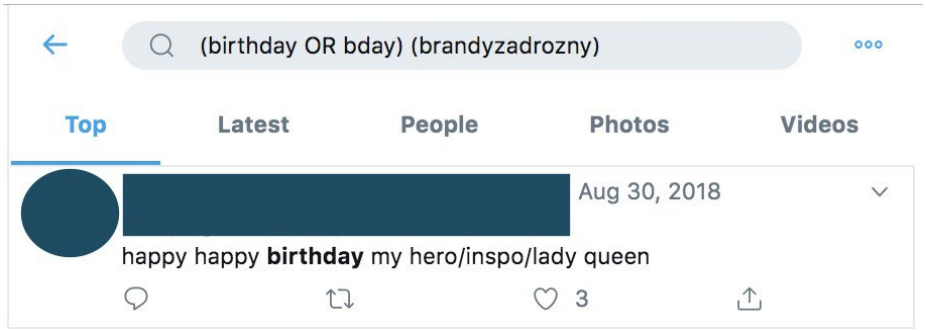


Qeni nuk ishte detaji i vetëm i dobishëm në imazhin e mëparshëm. Ai imazh erdhi nga babai i sulmuesit në Ohajo, dhe na ndihmoi të verifikonim llogaritë e tij personale dhe ato që i përkisnin familjes së tij.

Nëse keni një llogari në Facebook ose Twitter, është shumë e mundshme t'ju tregoj ditën kur keni lindur, edhe nëse nuk e ndani atë në profilin tuaj ose nuk postoni vetë për të. Meqenëse data e lindjes është shpesh një nga pjesët e para identifikuese të informacionit të dhënë nga policia në situatat e lajmeve të fundit (breaking news), një mënyrë e besueshme për të verifikuar një llogari të mediave sociale është të lëvizet në muajin dhe ditën në fjalë në një llogari të dyshuar dhe duke kërkuar për urimet e ditëlindjes. Edhe nëse faqet e tyre janë të zbrazëta, shpeshherë nënat dhe baballarët (si më sipër i Konor Bets-it) do të postojnë për ditëlindjet e fëmijëve të tyre.

E njëjta gjë vlen edhe për Twitterin, sepse, kujt nuk i pëlqen ditëlindja?

Mirëpo, është edhe më e lehtë të gjesh një postim identifikues në Twitter, sepse mjeti i tij i avancuar i kërkimit është ndër më të mirët që ofrohen nga platformat sociale. Edhe pse rrallë e lajmëroj ditëlindjen time, nëse e bëj fare, arrita të gjej një tuit ditëlindjeje nga një koleg i dashur që më ka zbuluar.



Ditëlindjet janë vetëm një shembull. Dasmat, funeralet, festat, përvjetorët, diplomimet - pothuajse çdo shënues kryesor i jetës festohet në mediat sociale. Këto ofrojnë një hapje për kërkimin dhe hetimin e një llogarie.

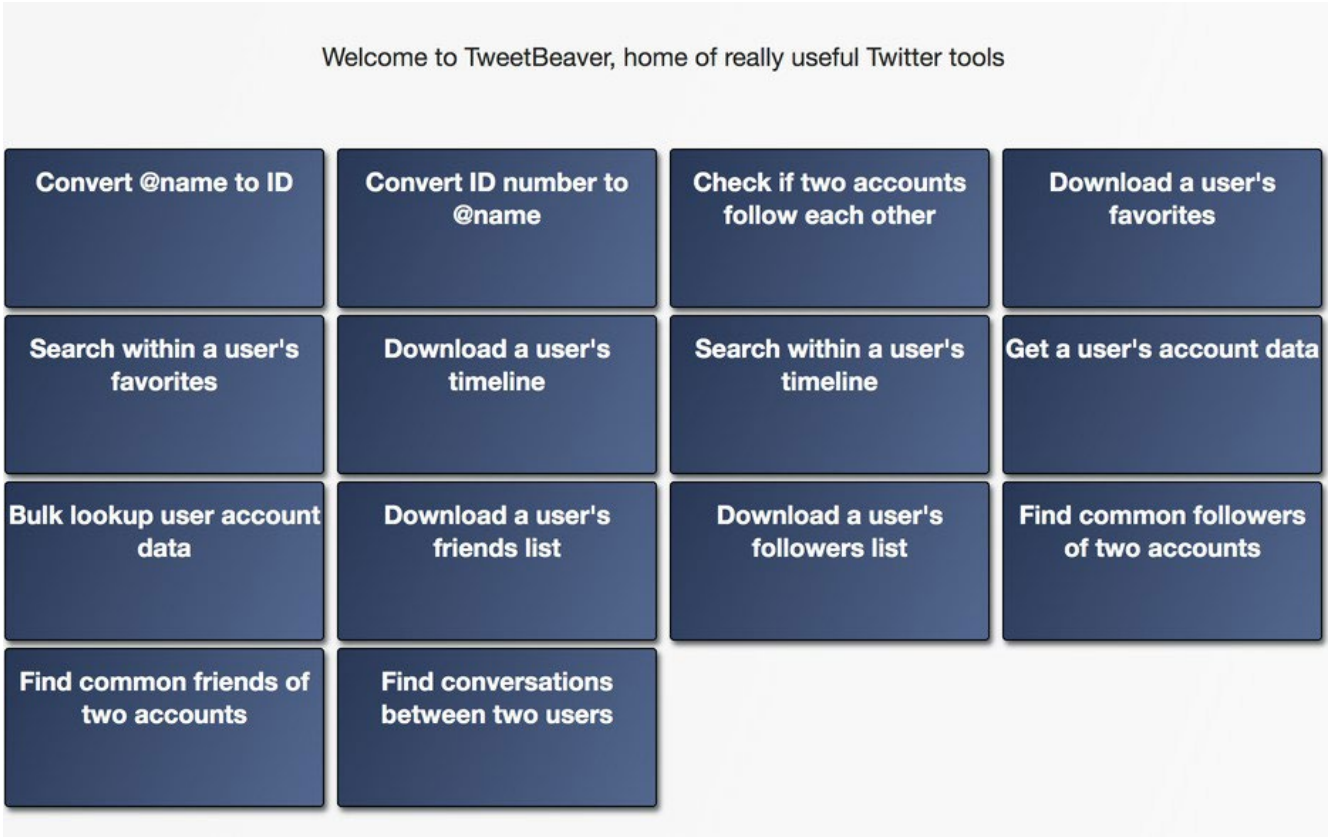
Mund të kërkoni për këto fjalë kyçe edhe përmes filtrave të tjera me mjetet e kërkimit në Facebook. Ata nuk përdoren aq sikurse para lëvizjes së platformës drejt privatësisë, por ekzistojnë ende. Një nga faqet e mia të preferuara është whopostedwhat.com.

Marrëdhëniet

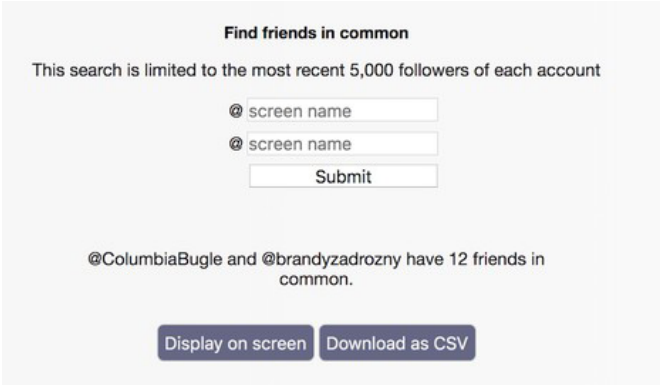
Mund ta gjykoni një person sipas shoqërisë që ka në rrjetet sociale. Mund të kuptojmë shumë për jetën dhe prirjet e një personi duke ekzaminuar njerëzit me të cilët ndërvepron onlajn.

Kur hapa llogari në Twitter për herë të parë, e nxita edhe burrin dhe shokun më të ngushtë të regjistroheshin gjithashtu, vetëm që të mund të më ndiqnin. Mendoj për atë kur po kërkoj llogaritë për punën time. Platformat nuk duan që të jesh i vetmuar, prandaj kur hap llogari së pari, aktivizohet një algoritëm. I ndikuar nga lista e kontakteve në telefonin tuaj, paraqitja juaj në listat e kontakteve të llogarive ekzistuese, lokacioni juaj dhe faktorët tjerë, platforma do t'ju sugjerojë llogari për t'i ndjekur.

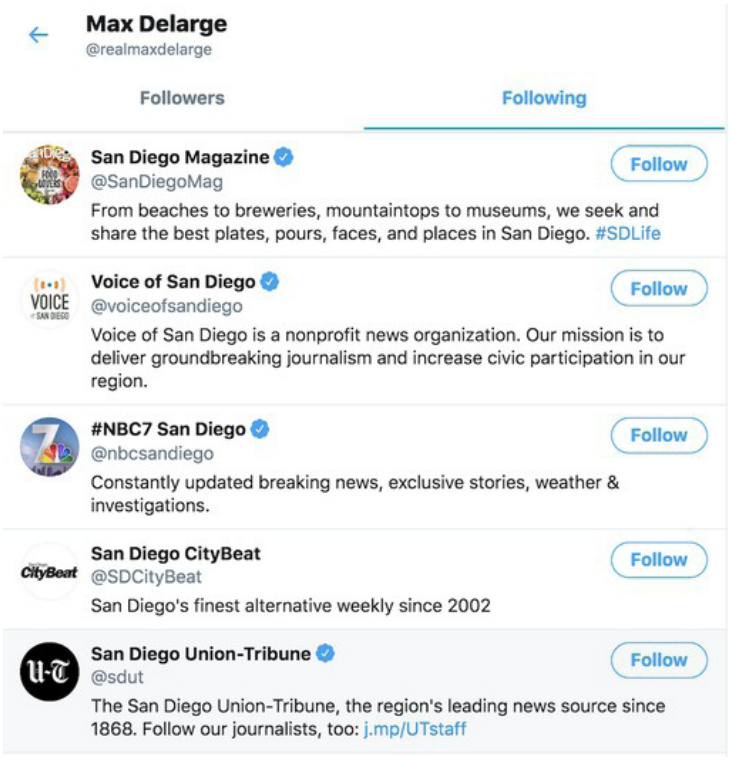
Për shkak të kësaj të vërtete, është gjithmonë iluminuese të shikosh ndjekësit dhe miqtë më të hershëm të një llogarie. TweetBeaver është një mjet i mirë për të hetuar lidhjet midis llogarive të mëdha dhe për të shkarkuar gjëra si tajmlajnet (timelines) dhe të preferuarat e llogarive më të vogla. Për grupe të dhënash më të mëdha, mbështetem te një zhvillues (developer) me qasje në API.

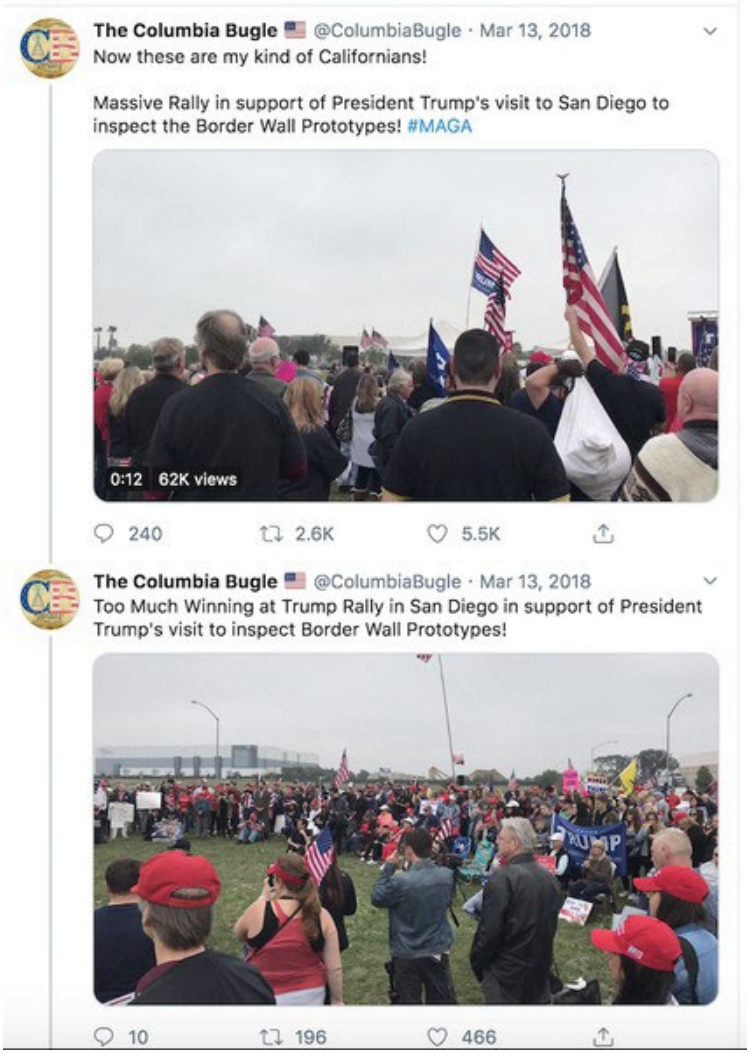


Le të marrim si shembull The Columbia Bugle, një llogari e njohur anonime e së djathtës ekstreme në Twitter që mburret se është rituituar dy herë nga llogaria e Donald Trampit.

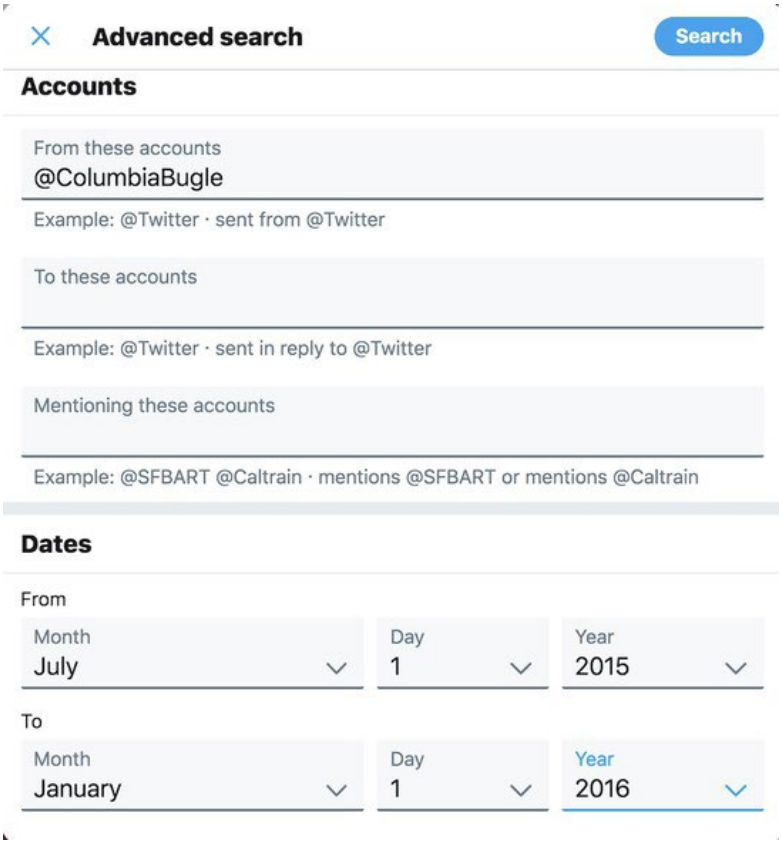


Ndjekjet më të hershme të Maks Delarxh (Max Delarge), një llogari që pretendon të jetë redaktori i The Columbia Bugle, janë burime lajmesh specifike për San Diegon dhe llogari sportive specifike për San Diegon. Meqenëse shumë prej postimeve të Columbia Bugle përfshijnë video nga tubimet dhe ngjarjet të Trampit në Universitetin e Kalifornisë në San Diego, mund të jemi mjaft të sigurt se personi që qëndron pas llogarisë jeton afër San Diegos.

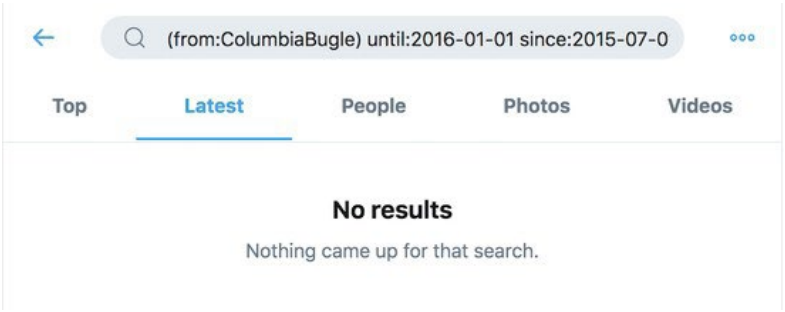




Gjatë një hetimi të ri, më pëlqen të filloj në fillim të Twitter historisë së dikujt dhe të punoj duke shkuar përpara në kohë. Mund të arrish atje në mënyrë manuale, me ndihmë të ekstensionit "autoskroller" për Chrome, ose mund të përdorësh kërkimin e avancuar të Twitterit për të ku-fizuar kornizën kohore në muajt e parë të ekzistimit së një llogarie.



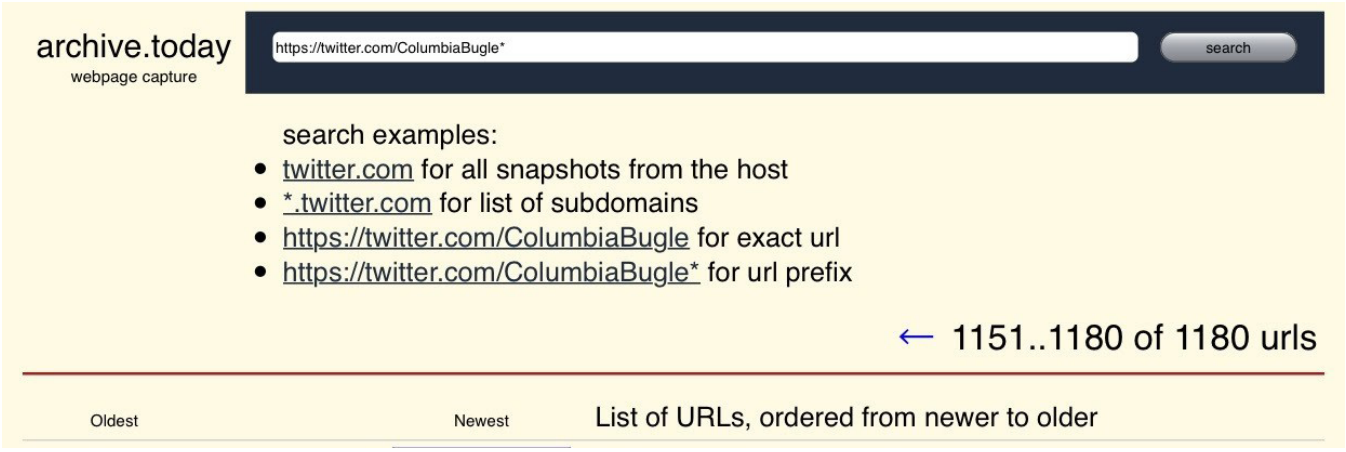
Çuditërisht, gjashtë muajt e parë të kësaj llogarie shfaqin zero tuite.



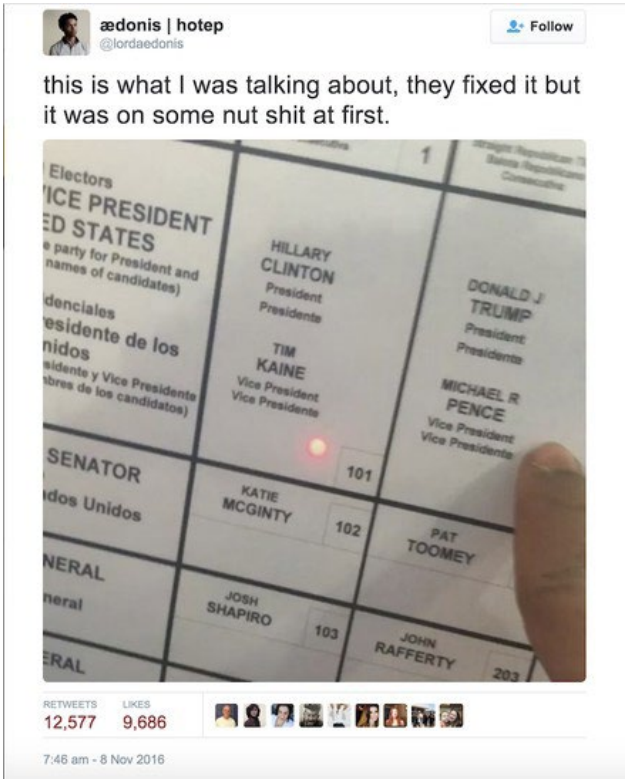
Kjo sugjeron që personi që qëndron pas The Columbia Bugle mund të ketë fshirë tuitet e tij të mëparshme. Për të zbuluar pse mund të ketë ndodhur kjo, unë mund ta ndryshoj kërkimin tim. Në vend të tuiteve nga llogaria, do të kërkoj çfarëdo tuiti që përmend The Columbia Bugle.

Këto biseda konfirmojnë se Columbia Bugle ka fshirë vitin e parë të tuiteve, por nuk na tregon pse dhe llogaritë e para me të cilat ka ndërvepruar kjo llogari nuk ofrojnë shumë gjurmë.

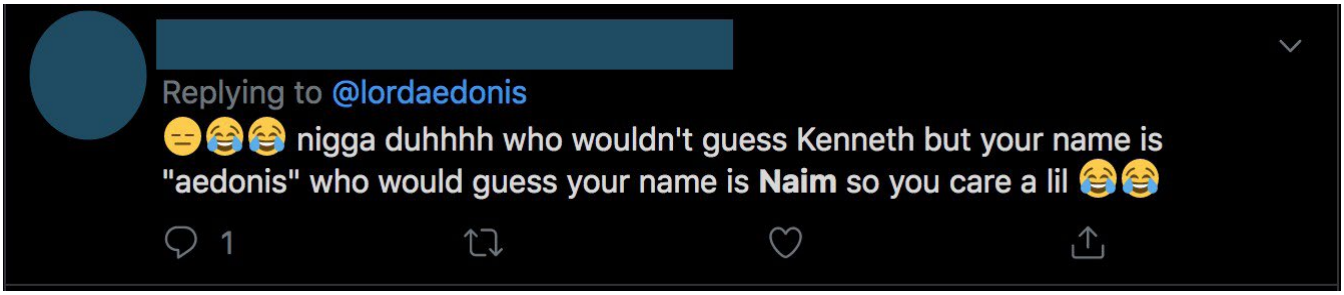
Për t'i gjetur tuitet e fshira së fundmi, mund të kërkoni në cache të Google; Tuitet e vjetra shpesh mund të jenë të qasshme në Wayback Machine të Arkivit të Internetit, ose në arkiv tjetër. Faqja e arkivave manuale archive.is shfaq disa tuite të fshira nga ku kuptohet se Columbia Bugle mori pjesë në një ngjarje ku studentët e kolegjit shkruanin mesazhe pro-Trampit në kampuset e tyre. Për t'i parë të gjitha tuitet që dikush mund t'i ketë arkivuar nga ajo llogari, siç bëra unë për ta gjetur këtë tuit, mund të kërkoni sipas prefiksit të URL-së, duke përdorur një yll pas emrit të llogarisë në këtë mënyrë:



Është e rrallë që dikush ta mbajë me sukses jetën e tij reale të ndarë nga aktivitetet e tij në internet. Për shembull, kolegu im në NBC News dhe unë treguam storien për pretendimin më viral dhe më mashtrues të vitit 2016 - për mashtrim të votuesve në ditën e zgjedhjeve, me ndihmën e një njeriu nga lagjja që njihte një troll të ekstremit të djathtë që e postoi këtë pretendim në Twitter.



Megjithëse tuiti buronte nga një njeri i njohur për ndjekësit e tij si @lordaedonis, njerëzit nga lagjja e tij aktuale u ishin përgjigjur postimeve të mëparshme me emrin e tij të vërtetë, të cilin e përfshimë në profilin e një sipërmarrësi të uritur për vëmendje, tuiti i të cilit u përhap nga një llogari në Twitter e mbështetur nga Kremlini, dhe që eventualisht u pa nga miliona përdorues dhe u promovua nga ai që së shpejti pas kësaj u bë president.



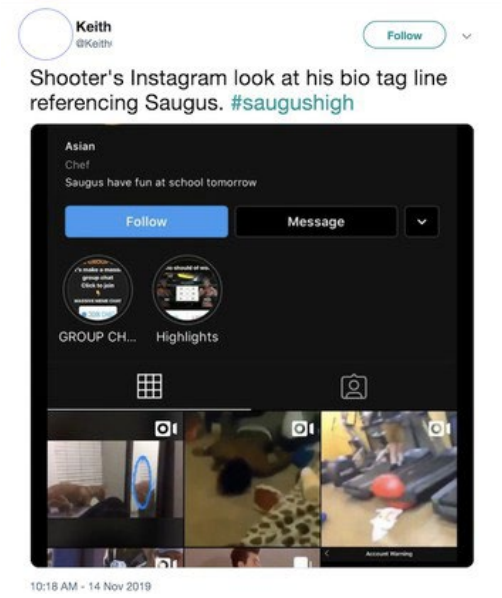
Konfirmimi i një llogarie sociale me subjektin, familjen dhe miqtë, zbatimin e ligjit dhe/ose PR-in e mediave sociale janë mënyra për të mbrojtur veten nga mashtrimi.

Llojet e mia të preferuara të storieve janë ato që zbulojnë njerëzit e vërtetë që qëndrojnë pas llogarive anonime me ndikim në mediat sociale. Këto llogari sekrete janë më pak të varura nga algoritmi dhe janë krijuar më me kujdes për të qenë një ikje nga jeta publike. Ata i lejojnë dikujt që të mbajë kontakt dhe të komunikojë me familjen dhe miqtë veçmas nga llogaria e tyre publike, ose të komunikojë ide dhe opinione që për arsye personale ose politike, nuk guxon t'i thotë hapur.

Gazetarja Eshli Fejberg është zana - kumbarë e këtyre llojeve të storieve tërheqëse, ato që demaskojnë alt-llogaritë e figurave të rëndësishme si Xhejms Komi ose Mit Romni. Sekreti i saj ishte thjesht çështje e gjetjes së llogarive më të vogla të anëtarëve të familjes që Komi dhe Romni natyrisht do të dëshironin t'i ndiqnin, e më pas të skrollonte nëpër to derisa gjeti një llogari që dukej joautentike, por përmbajtja dhe rrjeti i miqve/ndjekësve i së cilës përputheshin me atë të këtyre njerëzve të vërtetë.

Keni kujdes me llogaritë e rreme

Çdo platformë ka personalitetin e saj, aftësitë e kërkimit dhe dobinë në situata të ndryshme të lajmeve. Por, një fjalë kujdesi lidhur me llogaritë në media sociale: Zbatohet po të njëjta rregull "beso por verifiko". Ka grupe njerëzish që kënaqen kur mashtrojnë gazetarët. Sidomos në situatat e lajmeve të fundit, do të lindin gjithmonë llogari të rreme, shumë prej tyre me postime ogurzeza ose kërcënuese që synojnë të tërheqin gazetarët. Kjo llogari e rreme në Instagram përdorte emrin e një gjuajtësi masiv dhe u krijua pas gjuajtjes në shkollën e mesme Saugus në Kaliforni. Ajo fitoi vëmendjen përmes skrinshoteve në Twitter, por BuzzFeed News më vonë zbuloi se nuk i përkiste sulmuesit.



Në fund, e ndoshta edhe shënimi më i rëndësishëm: Nuk ka asnjë rend të duhur për të përfunduar këto hapa. Shpesh, më çojnë poshtë vrimave të lepurit dhe kam aq shumë tabe (skeda) të hapura që nuk më bën krenare. Krijimi i një sistemi që mund ta replikoni – qoftë nëse është mbajtja e evidencës së hapave tuaj në një dokument të Google ose lejimi i një vegle me pagesë si Hunchly që të monitorojë ndërsa kërkoni – është kyçe për të qartësuar lidhjet midis njerëzve dhe jetëve që ata bëjnë onlajn, si dhe për t'i kthyer ato përfundime në storie.

1a. Rast studimi:
Si hetimi i një sërë llogarish në Facebook zbuloi një përpjekje të koordinuar për të përhapur propagandë në Filipine

Shkruajnë: Vernis Tantuko and Gema Bagajaua-Mendoza

Një gazetare profesioniste për rreth 20 vjet, **Gema Bagajaua-Mendoza** *(Gemma Bagayaua-Mendoza) është drejtuese e kërkimit dhe strategjisë në Rappler. Ajo drejton njësinë e kontrollit të fakteve, si dhe hulumtimin e Rappler për dezinformatat dhe misinformatat (informatat e gabuara) në internet*

Vernis Tantuko *(Vernise Tantuco) është anëtare e ekipit hulumtues të Rappler, ku punon në kontrollet e fakteve dhe studion rrjetet e dezinformimit në Filipine*

Në vjeshtën e vitit 2016, John Victorino, një analist investimesh, i dërgoi Rappler-it një listë të asaj që ai tha se ishin 26 llogari të dyshimta në Facebook nga Filipinet. E filluam hetimin dhe monitorimin e llogarive dhe shpejt zbuluam se detajet e listuara në profilet e tyre ishin të rreme. Gjatë javëve të hetimit, këto 26 llogari na çuan të zbulonim një rrjet shumë më ekstensiv faqesh, grupesh dhe llogarish.

Këto llogari, së bashku me një grup faqesh dhe grupesh me të cilat ishin lidhur, u hoqën për-fundimisht nga Facebook. Ata gjithashtu e frymëzuan Rappler-in për të krijuar Sharktank-un, një mjet për të monitoruar se si rrjedh informacioni në Facebook. Kjo punë formoi bazën e një sërë storiesh hulumtuese rreth asaj se si propaganda dhe operacionet e informacionit në Facebook ndikojnë në demokracinë në Filipine. Seria përfshinte një hetim mbi aktivitetet e 26 llogarive të rreme dhe filloi mbulimin tonë të vazhdueshëm se si Facebook është përdorur në Filipine si armë për të përhapur dezinformata politike, për të sulmuar njerëz dhe për të minuar demokracinë në vend.

Ky rast studimi shqyrton se si hetuam 26 llogaritë origjinale dhe i përdorëm ato për të zbuluar rrjete shumë më të mëdha.

Verifikimi i identiteteve, ekspozimi i kukullave

Hapi ynë i parë në hetimin e grupit të llogarive ishte përpjekja për të verifikuar nëse ato ishin të lidhura me njerëz të vërtetë. Kjo pjesë kërkonte një kontroll të mirë faktesh në mënyrë tradicionale dhe filloi me krijimin tonë të fletëllogaritësve (spreadsheets) për të ndjekur detajet në lidhje me llogaritë, duke përfshirë detajet personale që kanë listuar, faqet që kanë pëlqyer dhe informacione të tjera.

Për shembull, përdoruesja e Facebook-ut Mutya Bautista e përshkroi veten si një "analiste softuerike" në ABS-CBN, rrjetin më të madh televiziv të Filipineve. Rappler e kontrolloi këtë me ABS-CBN, i cili konfirmoi se ajo nuk punonte për ta.

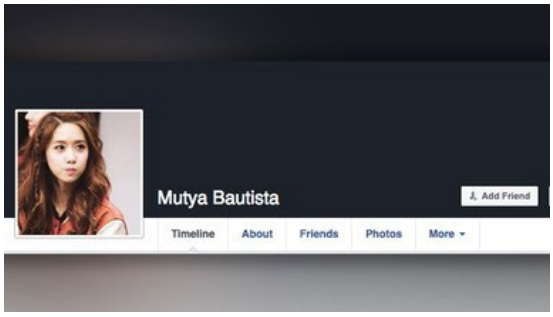
Personal Information	
Facebook ID	https://www.facebook.com/profile.php?id=10
Profile Name	Mutya Bautista
Occupation	Software Analyst
Current Company	ABS-CBN Corporation
Former Occupation 1	
Former Occupation 2	
Former Occupation 3	
Former Occupation 4	
Former Occupation 5	
Studied	Computer Engineering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

Duke përdorur mjetet e kërkimit të kundërt të imazheve, zbuluam se shumë nga 26 llogaritë kanë përdorur fotografi të profilit të personave ose personaliteteve të famshëm.

Bautista, për shembull, ka përdorur një foto të Im Yoona të pop grupit korean Girl's Generation. Llogaria e Lily Lopez, e paraqitur më poshtë, ka përdorur imazhin e aktores koreane Kim Sa-rang.



Një llogari tjetër, Luvimin Cancio, ka përdorur një imazh nga softcorecams.com, një faqe pornografike, si foto të profilit të saj. Ne e identifikuam këtë faqe interneti si burimin e fotografisë përmes mjetit të kërkimit të imazhit të kundërt TinEye.

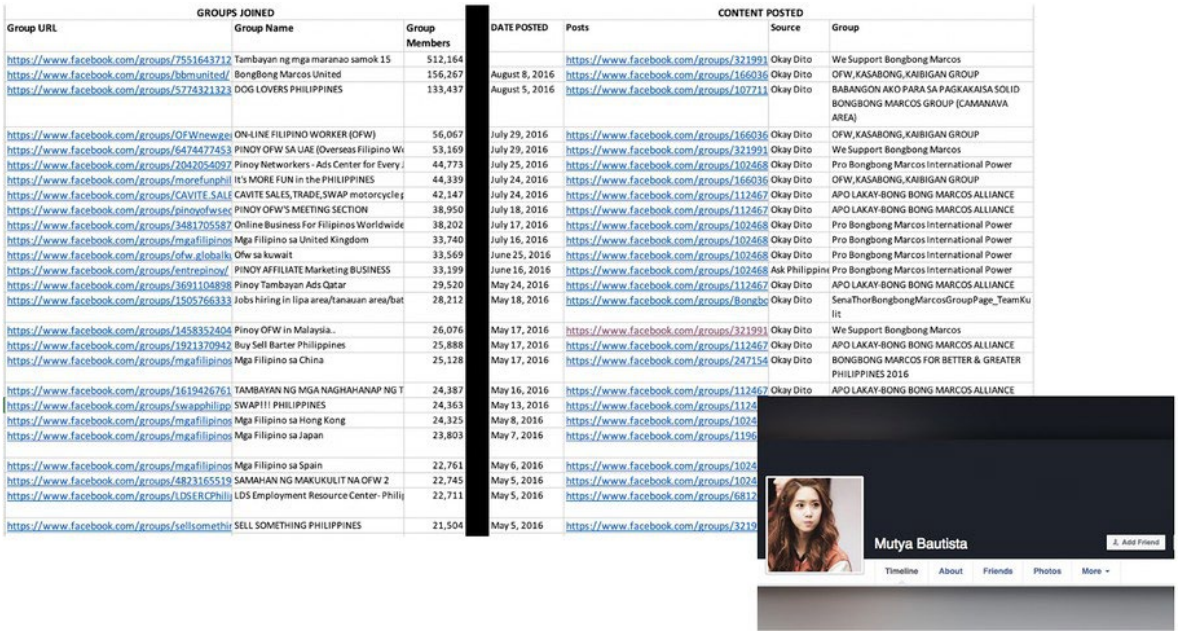
Llogaritë gjithashtu përdorën cover-foto (foto në krye të profilit) të ngjashme në profilet e tyre. Më poshtë, cover-fotografia e llogarisë së Jasmin De La Torre është e njëjtë me atë të Lily Lopez.

Gjithashtu, vumë re një gjë kurioze për 26 llogaritë: Këta përdorues kishin më shumë grupe sesa miq.

Kjo ishte e pazakontë sepse, në Filipine, shumica e njerëzve kanë miq dhe familje jashtë vendit. Facebook në thelb shërben si kanal komunikimi përmes të cilit njerëzit mbajnë kontakte me familjen dhe miqtë. Pra, ata më shumë priren të kenë shumë miq sesa të jenë anëtarë të një numri të madh grupesh.

Lista e miqve të Bautista-s, e cila ishte publike në atë kohë, tregonte se ajo kishte vetëm 17 miq. Në fakt, kur i zbuluam në vitin 2016, secila nga 26 llogaritë që i identifikuam kishte më pak se 50 miq.

Megjithatë, Bautista ishte anëtare e mbi njëqind grupeve, duke përfshirë grupe që bënin fushatë për kandidatin e atëhershëm për zëvendës-president, Ferdinand Markos i Riu., një numër komunitetesh filipinase jashtë shtetit, si dhe grupe për shitblerje, secili me anëtarë që silleshin nga dhjetëra mijëra deri në qindra mijëra. Në total, këto grupe kanë mbi 2.3 milionë anëtarë në Facebook. Më poshtë është një listë e disa prej grupeve më të mëdha, duke përfshirë numrin e ndjekësve të tyre. Është gjithashtu e përfshirë një listë e postimeve që Bautista ka bërë në këto grupe.



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	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.globalks	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		

Duke kombinuar të gjitha këto vëzhgime dhe të dhëna shoqëruese, arritëm në përfundimin se llogaritë ishin kukulla: identitete imagjinare të krijuara për të forcuar një këndvështrim të veçantë.

Rrjeti pro-Markos

Nga datat e lidhura me fotot e para të profilit dhe postimet e hershme të këtyre 26 llogarive mund të shihnim se ato dukej se ishin krijuar në tremujorin e fundit të 2015, e deri në zgjedhjet e majit 2016. Gjithashtu zbuluam se ato vazhdimisht promovonin përmbajtje që mohonin abuzimet e dokumentuara gjerësisht të ligjit ushtarak që ndodhën në vitet 1970 nën regjimin e Markosit. Llogaritë po ashtu sulmuan rivalët e të birit të ish-diktatorit, kandidat për zëvendës-president, Ferdinand "Bongbong" Markos i Riu.

Në shembullin e mëposhtëm, përdoruesja Mutya Bautista shpërndau një pretendim tashmë të përgënjeshtruar se rivali i Bongbong, zëvendës-presidenti i saposhpallur në atë kohë Leni Robredo, ishte martuar më parë me një aktiviste përpara se ajo të martohej me burrin e saj të dytë, sekretarin e ndjerë të Brendshëm dhe të qeverisë lokale, Jesse Robredo. Bautista postoi artikullin me titull "Leni Robredo ishte martuar me një adoleshente anti-Markos përpara se të takonte Jesse?" në grupin "Pro Bongbong Marcos International Power", me komentin: "Kaya ganun na lamang ang pamemersonal kay [Bongbong Marcos], may root cause pala." ("Kjo është arsyeja pse është personale kundër [Bongbong Marcos], ka një shkak rrënjësor.")

Një tjetër llogari e dyshimtë me emrin Raden Alfaro Payas e shpërndau të njëjtin artikull në grupin "Luftëtarët besnikë të Facebook-ut të Bongbong Markos"("Bongbong Marcos loyalist Facebook warriors") me të njëjtin titull - fjalë për fjalë, deri në shenjën e fundit të pikësimit - në të njëjtën ditë.

Llogaritë e rreme përdoren shpesh për të spamuar grupe me linqe, dhe ndonjëherë mund t'i kapni duke ripërdorur të njëjtin tekst kur e bëjnë atë. Në atë kohë, ishte e mundur të përdorej kërkimi i grafikut në Facebook (Facebook Graph search) për të parë postimet publike të përdoruesve në grupe. Mirëpo, Facebook mbylli shumë veçori të kërkimit Graph në vitin 2019, duke përfshirë edhe këtë funksion. Si rezultat, tani është e nevojshme të shkosh në grupe dhe të kërkosh për të parë se çfarë kanë shpërndarë përdorues të veçantë.

Uebfaqe të lidhura

Duke analizuar se çfarë përmbajtje kenë shpërndarë llogaritë, patëm mundësi të shohim se 26 kukullat po promovonin të njëjtat uebfaqe: Okay Dito (0KD2.com), Ask Philippines (askphilippines.com) dhe WhyOwhy.com, ndër të tjera.

OKD2.com ka publikuar një sërë mashtrimesh dhe materiale të tjera propagandistike që favorizojnë familjen Markos dhe presidentin Rodrigo Duterte. Tani ajo maskohet si një faqe reklamash të klasifikuara. Por në shtator 2016 zbuluam se përmbajtjet nga faqja janë shpërndarë 11.900 herë në Facebook, pjesërisht falë kukullave.

Nëpërmjet këtyre uebfaqeve, Rappler përfundimisht ra në gjurmë të mjeshtrit të mundshëm të kukullave të 26 llogarive: personit me emrin Raden Alfaro Payas.

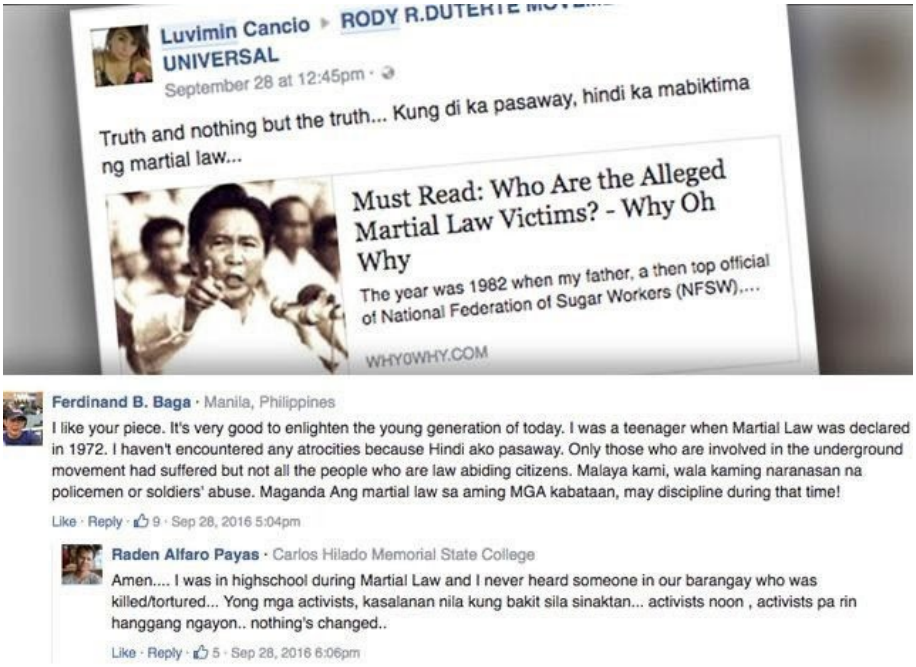
Gjurmimi i mjeshtërve të kukullave

Ashtu si shumë sajte që monitoron Rappler, të dhënat aktuale të regjistrimit të domenit të OKD2.com janë private. Sajti gjithashtu nuk zbulon autorët ose pronarët e tij dhe nuk ka asnjë informacion kontakti përveç një ueb formulari.

Për fat të mirë, ne ishim në gjendje të përdorim të dhënat historike të domenit për të identifikuar një person të lidhur me sajtin. Duke përdorur domaintools.com, mund të shihnim se që nga korriku 2015, OKD2.com ishte regjistruar në emër të personit Raden Payas, një banor i qytetit Tanauan, Batangas. Zbuluam gjithashtu se 0KD2.com ndante të njëjtën ID të Google AdSense si uebfaqe tjera, si për shembull askphilippines.com dhe WhyOwhy.com, të cilat po ashtu shpërndaheshin nga 26 llogaritë. I identifikuam ID-të e AdSense në këto sajte duke parë kodin burimor të faqeve në to dhe duke kërkuar një seri numrash që fillonin me shkronjat "ca-pub-". Secilës llogari të Google AdSense i jepet një ID unike që fillon me "ca-pub-," dhe çdo faqe e një sajti që është e lidhur me një llogari do ta ketë në të këtë kod.

Së bashku me regjistrimin e domenit, pamë gjithashtu se një nga 26 llogaritë quhej Raden Alfaro Payas (jozyrtare). Gjithashtu, gjetëm një llogari tjetër në emrin e tij me emrin e përdoruesit "realradenpayas", i cili ndërvepronte me disa nga kukullat.

Për shembull, ai komentoi në një postim nga Luvimin Cancio që lidhej me një storie që mohonte mizoritë e ligjit ushtarak gjatë sundimit të Markosit. Llogaria "e vërtetë" e Payas thoshte se ai ka qenë në shkollë të mesme gjatë viteve të ligjit ushtarak dhe se ai "asnjëherë nuk kishte dëgjuar" që dikush të ishte vrarë apo torturuar.



Krijimi i Sharktank

Këto 26 llogari të rreme dhe shtrirja (reach) e tyre frymëzuan Rappler për të krijuar bazën e tij të të dhënave Sharktank dhe për të automatizuar mbledhjen e të dhënave nga Facebook grupet dhe faqet publike. Që nga gushti i vitit 2019, Rappler ka gjurmuar afërsisht 40,000 faqe me miliona ndjekës.

Ajo që filloi si një hetim i një sëre të llogarive të dyshimta u shndërrua në një studim të vazhdueshëm të një rrjeti me mijëra llogari të rreme dhe reale, grupe dhe faqe që përhapin dezinformata dhe propagandë, që bëjnë shtrembërime politike dhe dobësojnë demokracinë e një kombi.

1b. Rast studimi:
Si vërtetuam se faqja më e madhe e Black Lives Matter në Facebook ishte e rreme

Shkruan: Doni O'Salliven

Doni O'Salliven *(Donie O'Sullivan) është reporter i CNN që mbulon kryqëzimin e teknologjisë dhe politikës. Ai është pjesë e ekipit të CNN Business dhe bashkëpunon ngushtë me njësinë hulumtuese të CNN për gjurmimin dhe identifikimin e fushatave të dezinformimit në internet që shënjestrojnë elektoratin amerikan.*

Në verën dhe vjeshtën e vitit 2017, ndërsa bota filloi të mësonte detajet e përpjekjeve ekspansive të Rusisë për të ndikuar tek votuesit amerikanë përmes mediave sociale, u bë e qartë se afrikano-amerikanët dhe lëvizja Black Lives Matter ishin ndër caqet kryesore të fushatës së Kremlinit për të mbjellë ndarje.

Kolegët e mi në CNN dhe unë kaluam muaj duke raportuar se si Rusia kishte qenë prapa disa prej llogarive më të mëdha të Black Lives Matter (BLM) në mediat sociale. Ndërsa flisja me aktivistët e BLM, ndonjëherë më pyesnin: "A e dini se kush drejton faqen më të madhe Black Lives Matter në Facebook?"

Çuditërisht, askush - duke përfshirë aktivistët më të shquar të BLM në vend dhe organizatorët në terren - nuk e dinte përgjigjen. Disa kishin dyshime të kuptueshme se faqja mund të drejtohej nga Rusia. Mirëpo, hetimi ynë zbuloi se nuk ishte rus apo amerikan – ajo drejtohej nga një njeri i bardhë në Australi.

Faqja, e titulluar thjesht " Black Lives Matter", dukej legjitime. Që nga prilli i vitit 2018, ajo kishte pothuajse 700,000 ndjekës. Ajo shpërndante vazhdimisht linqe të storieve për brutalitetin policor dhe pabarazinë; ajo organizonte mbledhje fondesh onlajn; madje kishte edhe një shitore onlajn që shiste BLM mallra.

Nuk është e pazakontë që një faqe me atë madhësi të drejtohet në mënyrë anonime. Disa aktivistë nuk duan t'i vendosin emrat e tyre në një faqe dhe të rrezikojnë të tërheqin vëmendjen nga trollët ose nga forcat e ligjit që kërkojnë të shuajnë protestat. Jashtë SHBA-ve, aftësia e aktivistëve për të drejtuar faqet në mënyrë anonime ka qenë kritike për aktivizmin digjital dhe kyçe për disa lëvizje. (Mu këtë e shfrytëzoi Rusia, duke shtuar dyshimet se ky BLM ishte e lidhur.)

Rreth kohës kur fillova t'i kushtoja vëmendje kësaj faqeje misterioze, Jeremy Massler, hulumtues i pavarur dhe një hetues i jashtëzakonshëm onlajn, mu qas me një këshillë. Massler kishte parë të dhënat e regjistrimit të domenit të uebfaqeve, me të cilat lidhej vazhdimisht faqja e madhe BLM në Facebook. Edhe pse domenet ishin regjistruar privatisht, ai zbuloi se një prej tyre, për një periudhë në vitin 2016, i përkiste një personi në Pert, Australi, i quajtur Ian MacKay - një burrë i bardhë.

```
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
```

Massler kontaktoi me MacKay, i cili i tha se ai blinte dhe shiste domene si një hobi dhe nuk kishte asnjë lidhje me faqen në Facebook. Ishte i njëjti justifikim që më dha MacKay, një zyrtar i sindikatës në moshë të mesme, kur e kontaktova me telefon disa muaj më vonë. Mirëpo, deri në atë kohë, ne kishim zbuluar se MacKay kishte regjistruar dhjetëra emra uebfaqesh, shumë prej tyre të lidhura me "aktivizmin e zi".

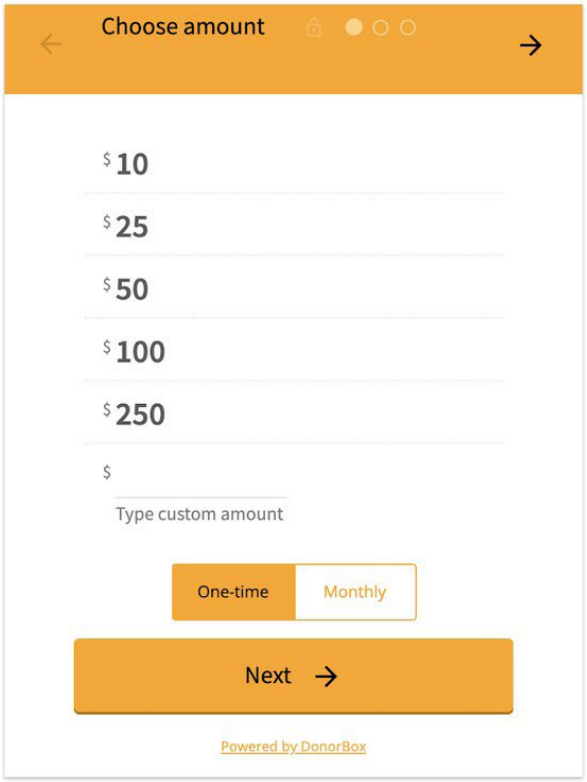
Pavarësisht shqetësimeve të mia për faqen dhe faktit që disa aktivistë më thanë se kishin dyshime për të, shpjegimi i MacKay nuk mu duk i pabesueshëm në dukje. Emrat e domenit mund të jenë të vlefshëm, dhe njerëzit i blejnë dhe i shesin vazhdimisht. Fakti që ai kishte regjistruar dhe shitur gjithashtu domene që nuk kishin lidhje me aktivizmin e zi, e bëri argumentimin e tij edhe më të besueshëm. Mirëpo, më pas ndodhi diçka e çuditshme. Disa minuta pasi fola me MacKay, faqja në Facebook ra. Nuk ishte hequr nga vetë Facebook-u, por nga kushdo që e drejtonte - dhe nuk ishte fshirë, vetëm ishte hequr përkohësisht.

Kjo dukej e dyshimtë, kështu që Mossier dhe unë filluam të gërmojmë më shumë.

Faqja në Facebook, e cila u kthye në onlajn në javët pas telefonatës sime me MacKay, gjatë ekzistimit të saj kishte promovuar fushata për mbledhjen e fondeve gjoja për kauzat e BLM.

Në një rast, ajo pretendonte se po mblidhte para për aktivistët në Memfis, Tenesi. Por kur fola me aktivistët atje, askush nuk dinte asgjë për mbledhjen e fondeve apo se ku mund të kishin shkuar paratë. Madje, aktivistë të tjerë na thanë se, duke dyshuar se ishte një mashtrim, ata e kishin raportuar faqen në Facebook. Por, kompania nuk kishte ndërmarrë asnjë veprim.

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!

Ndërsa fillova të kontaktoja platformat e shumta të pagesave dhe mbledhjes së fondeve onlajn që kishte përdorur faqja, ato kompani filluan të mënjanojnë thirrjet për grumbullim të fondeve, duke thënë se kishin thyer rregullat e tyre. Duke cituar rregullat për privatësinë e përdoruesve, asnjë nga kompanitë e pagesave nuk më dha publikisht informacion se ku po shkonin paratë. Kjo është një sfidë e zakonshme. Duke cituar politikat e tyre të privatësisë, platformat dhe shërbimet digjitale rrallëherë ua zbulojnë mediave emrat ose informacionet e kontaktit të mbajtësve të llogarive.

Më vonë, nga një burim që kishte njohuri për disa nga pagesat e përpunuara, mësova se të paktën një llogari ishte e lidhur me një llogari bankare dhe një adresë IP australiane. Një burim tjetër më tha se ishin mbledhur rreth 100,000 dollarë. Zhvillimi i burimeve në kompanitë e teknologjisë, të cilët janë të gatshëm t'ju tregojnë më shumë informacion publikisht sesa vetë kompania, po bëhet gjithnjë e më i rëndësishëm pasi shumë storie nuk mund të zbulohen thjesht duke përdorur informacione nga burimet e hapura, pasi mashtruesit dhe aktorët e këqij po bëhen më të sofistikuar.

Për këtë informacion kërkova nga Facebook që të jepte koment për storien dhe u thashë se kisha prova që faqja ishte e lidhur me Australinë, që kompanitë e pagesave i kishin hequr fushatat pas hetimeve që kishin bërë, dhe se ne e dinim se një pjesë e parave po shkonte në Australi. Një zëdhënës i Facebook tha se hetimi i platformës së mediave sociale "nuk tregoi asgjë që shkelte standardet tona të komunitetit (Community Standards)".

Vetëm pak para publikimit të stories sonë, dhe vetëm pasi ngrita shqetësimin tim për hetimin e Facebook dhe përgjigjen e zëdhënësit të kompanisë te një punonjës më i lartë i Facebook-ut, Facebook-u ndërmori masa dhe e hoqi faqen.

Sindikata e punëtorëve australianë ku punonte MacKay nisi një hetim të vetin pas raportimit të CNN. Deri në fund të javës, e kishte pushuar nga puna MacKay-in dhe një zyrtar të dytë, për të cilin tha se ishte gjithashtu i përfshirë në mashtrim.

Ajo që ishte veçanërisht e dukshme për këtë storie ishte grupi i teknikave që Massler dhe unë përdorëm për t'ia dalë mbanë. U mbështetëm shumë në faqet e arkivave si Wayback Machine që na lejonte të shihnim pamjen e uebfaqeve me të cilat faqja kishte vendosur lidhje dhe vetë faqen përpara se të vinte në radarin tonë. Kjo ishte veçanërisht e dobishme, sepse pasi Massler fillimisht kontaktoi MacKay, njerëzit që qëndronin prapa faqes filluan përpjekje për të mbuluar disa nga gjurmët e tyre.

Përdorëm gjithashtu shërbime që gjurmojnë regjistrimet e domenit, duke përfshirë DomainTools.com, për të hetuar sajtet që MacKay kishte regjistruar dhe gjithashtu për të gjetur detajet e kontaktit të tij të drejtpërdrejtë. Massler gjithashtu përdori ekstensivisht "Facebook Graph Search" (një mjet që nuk është më në dispozicion) për të gjurmuar llogaritë e rreme të Facebook profileve që ishin krijuar për të promovuar faqen në grupet në Facebook. Hulumtimi i informacionit me burim të hapur dhe përdorimi i mjeteve kërkimore onlajn, si ato që përdoren për t'u qasur në regjistrat e domenit, janë instrumente jetike – por nuk janë të vetmet.

Akti i thjeshtë i marrjes së telefonit për të folur me MacKay dhe zhvillimi i burimeve për të ofruar informacione që përndryshe nuk do të bëheshin publike – teknikat tradicionale të gazetarisë – ishin kritike në ekspozimin e këtij mashtrimi.

2. Gjetja e pacientit zero

Shkruan: Henk van Es

Hank van Es *(Henk van Ess) është vlerësues për Rrjetin Ndërkombëtar të Kontrollit të Fakteve të Poynter. Ai ka obsesion pas gjetjen e storieve në të dhëna. Van Es trajnon profesionistë të medias në mbarë botën në kërkimin në internet, mediat sociale dhe multimedia. Klientët e tij përfshijnë NBC News, BuzzFeed News, ITV, Global Witness, SRF, Axel Springer dhe shumë OJQ dhe universitete. Uebfaqet e tij whopostedwhat.com dhe graph.tips përdoren shumë për të filtruar mediat sociale. Ai është @henkvaness në Twitter.*

Për dekada, stjuardi kanadez Gaetan Dugas njihej si "Pacienti Zero", njeriu i parë që solli AIDS-n në Shtetet e Bashkuara. Kjo referencë, i cili u përforcua nga librat, filmat dhe raportet e panumërta të lajmeve, e bënë atë "arki-armikun e një epidemie që do të vriste përfundimisht më shumë se 700,000 njerëz në Amerikën e Veriut".

Por nuk ishte kështu. Bill Darrow, një hulumtues në Qendrat për Kontrollin dhe Parandalimin e Sëmundjeve, intervistoi Dugas dhe e paraqiti atë si "Pacient O, si në "Out-of-California."(-Jashtë-nga-Kalifornia). Së shpejti, kjo u lexua gabimisht si numri 0, duke shkaktuar një reagim zinxhiri të informatave të gabuara (misinformatave), që vazhdoi deri së voni.

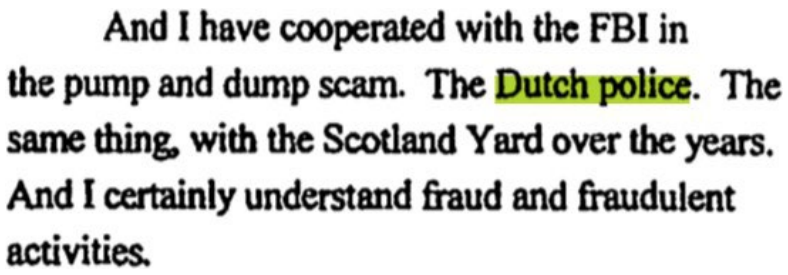
Është gjithashtu e mundur që një gazetar të fokusohet te pacienti i gabuar 0 nëse nuk dini si të kërkoni siç duhet. Ky kapitull ju ndihmon të gjeni burimet parësore (primare) onlajn duke hequr qafe rezultatet sipërfaqësore dhe duke gërmuar më thellë.

1. RREZIQET GJATË KONSULTIMIT TË BURIMEVE PARËSORE DHE MËNYRAT PËR T'I RREGULLUAR

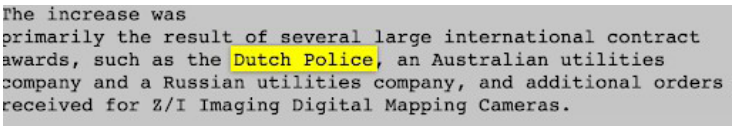
Gazetarët i duan burimet parësore në internet. Dëshmi të dorës së parë mund të gjenden në një artikull gazete, një studim shkencor, një komunikatë për shtyp, në mediat sociale ose në çdo "pacient zero" tjetër të mundshëm.

Kryerja e një kërkimi bazë të fjalëve kyçe në një faqe zyrtare të qeverisë mund t'ju bëjë të mendoni "ajo që shihni është ajo që e kanë". Kjo shpesh nuk është e vërtetë. Ja një shembull. Le të shkojmë te Komisioni për Siguri dhe Shkëmbim i SHBA-së (U.S. Securities and Exchange Commission), një burim që përdoret për të gjetur informacione financiare për qytetarët amerikanë, si dhe për njerëz të biznesit nga e gjithë bota. Le të themi se duam të gjejmë shfaqjen e parë të frazës "Policia holandeze" në sec.gov. Motori i integruar i kërkimit i SEC mund të ndihmojë:

Keni fituar vetëm një rezultat - një dokument nga viti 2016. Pra, SEC përmend policinë holandeze vetëm një herë, në vitin 2016, apo jo?


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.

E gabuar. Përmendja e parë në sec.gov ishte në vitin 2004, 12 vjet më parë, në një letër të deklasifikuar dhe të koduar:


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.

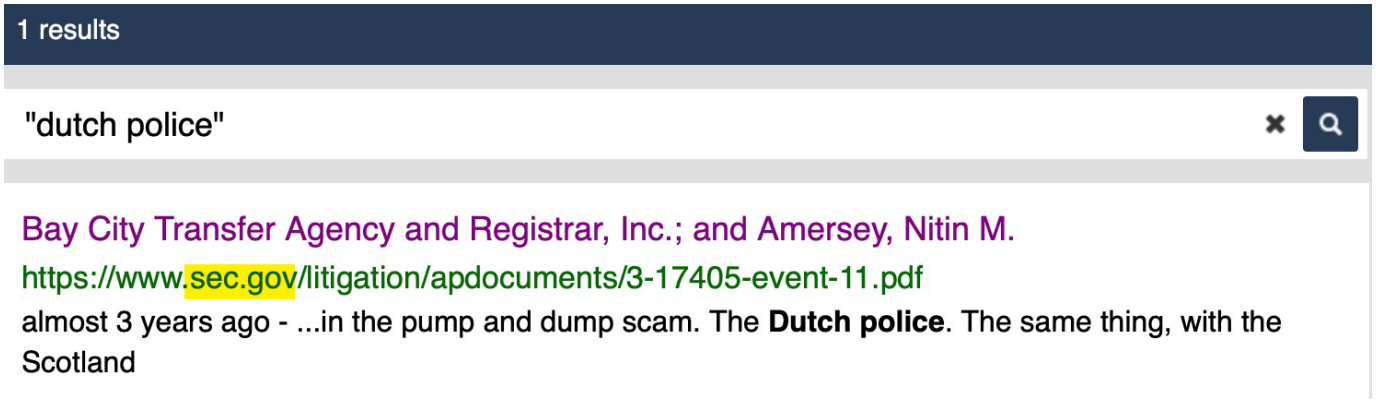
Këtë nuk do ta shihni në rezultatet e kërkimit nga shiriti për kërkim (search bar) në sec.gov, edhe pse ky informacion vjen drejtpërdrejt nga kjo uebfaqe. Pse është ky ndryshim?

Zakonisht, duhet të mos u besoni motorëve të kërkimit nga burimet primare. Ato mund t'ju japin një përshtypje të rreme të përmbajtjes aktuale të uebfaqes dhe bazave të të dhënave të lidhura me të. Mënyra e duhur për të kërkuar është të kryeni një "kontroll të burimit parësor" ("primary source check").

Kontrollimi i burimit parësor

Hapi 1: Shikojeni linkun e dështuar

Rezultati i kërkimit nga SEC na dha vetëm një burim:



Le të punojmë me këtë zhgënjim. Së pari, fshijeni "https://www", pjesën e parë të linkut. Kujdes te viza e pjerrët e parë pas kësaj (/) - në këtë rast është para fjalës "litigation/"

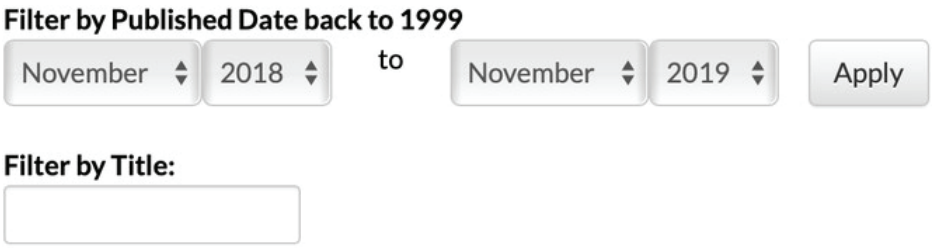
Kjo është pjesa që na duhet: sec.gov

Hapi 2: Përdorni "site:"

Shkoni te një motor kërkimi i përgjithshëm. Filloni me kërkimin "Dutch police" ("Policia holandeze") dhe përfundoni me "site:" e ndjekur drejtpërdrejt me URL-në (pa vende të zbrazëta). Kjo është formula për të zbuluar nëse një burim origjinal ju shfaq gjithçka:

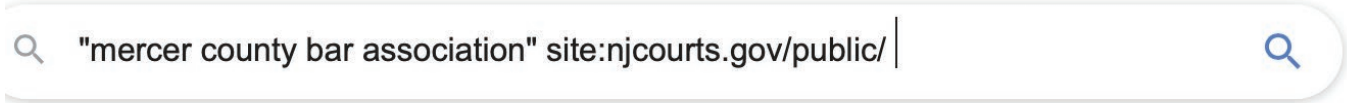
Përfshirja e folderëve specifikë

Tani mund të përshtatni "formulën e burimit primar" sipas nevojave tuaja. Le të shkojmë në seksionin e njoftimeve për shtyp të uebfaqes së Gjykatave të Nju Xhersit (New Jersey Courts). Të themi se dëshironi të mësoni se kur Shoqata e Avokatëve të Qarkut Mercer ka sponsorizuar një program të Ditës së Ligjit, por nuk mund ta gjeni burimin parësor në titullin e asnjë njoftimi për shtyp. "Dhoma e Avokatëve të Qarkut Mercer" nuk shfaqet në asnjë titull.



Tani shikoni URL-në e asaj faqeje plot me njoftime për shtyp të indeksuara dobët:

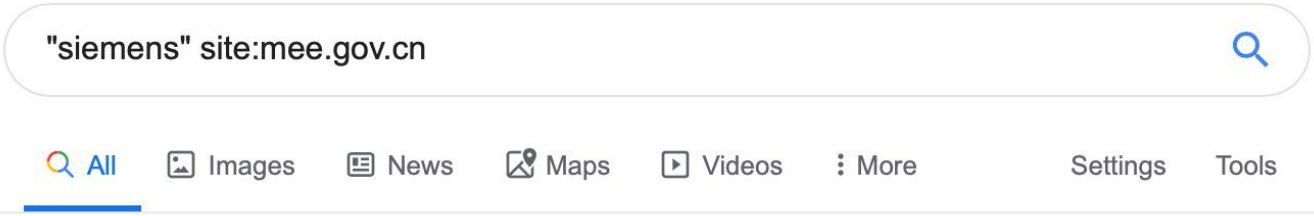
Materiali i marrëdhënieve me publikun ruhet në folderin /public. Kjo duhet të përfshihet në kërkimin tuaj në Google:



Dhe ja ku e keni:

Parashikimi i folderëve

Kina ka një Ministri të Ekologjisë dhe Mjedisit. A kanë dokumente angleze për kompaninë gjermane Siemens? Me formulën e mëposhtme, mund të gjeni dokumente ne gjuhën kineze dhe angleze në rezultatet e kërkimit:



Nëse doni të filtroni për të parë vetëm ato anglisht, ndoshta kanë përdorur fjalën anglisht në lidhje? Provojeni. Funksionon:

2. PËRCJELLJA E GJURMËVE TË DOKUMENTEVE

Ndonjëherë informacioni që na nevojitet nuk gjendet në një uebfaqe, por në fakt gjendet në një dokument të vendosur në një uebfaqe. Ja se si të ndiqni gjurmët e dokumentit duke përdorur formulat e Google.

Ross McKitrick është profesor i asociuar në Departamentin e Ekonomisë në Universitetin e Guelph, Ontario. Në vitin 2014, ai bëri një prezantim për një grup skeptik ndaj temave klimatike. Le të përpiqemi të gjejmë ftesën për atë takim. E dimë se është mbajtur më 13 maj 2014 dhe ishte Dreka e 11-të Vjetore e organizuar nga "Miqtë e Shkencës" ("Friends of Science (FOS)"). Nëse kërkojmë në Google për këto terma, dalim bosh:

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

Pse? Sepse fjala "ftesë" nuk gjendet në shumë ftesa. Është e njëjta gjë me fjalën "intervistë". Shumë intervista nuk e përmbajnë fjalën intervistë. Edhe shumica e hartave nuk e kanë fjalën hartë të shkruar në mënyrë eksplicite. Këshilla ime? Ndaloni së supozuari dhe përdorni Go Zen.

Hapi 1: Përcaktoni llojin e dokumentit

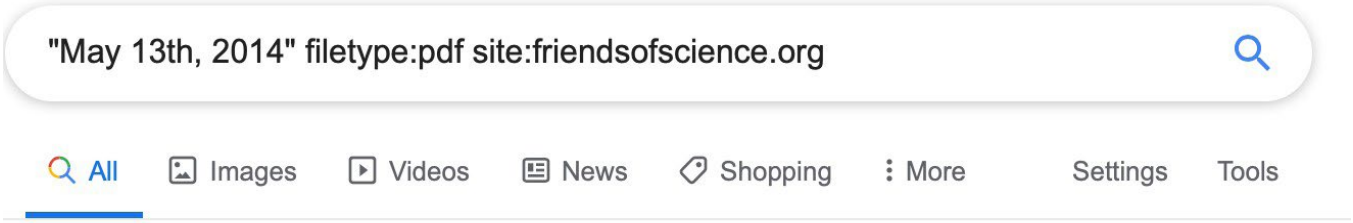
Mundohuni të gjeni emëruesin e përbashkët të çdo ftese në internet. Shpesh është një dokument PDF. Kërkoni vetëm atë me "filetype:pdf" dhe ndoshta mund ta gjeni.

Hapi 2: Bëhuni (klimatikisht) neutral

Nuk e dini formulimin e saktë të fjalëve në ftesë. Por ajo që dini është se videoja në YouTube ishte nga një ngjarje e 13 majit 2014. Është e mundur që data të përmendet në ftesë. (Sigurohuni që të kërkoni edhe format kardinale edhe ato rendore, 13 maj dhe maj 13)

Hapi 3: Kush është i përfshirë?

E dimë që organizatori është "Friends of Science" dhe se uebfaqja e tij është friendsofscience.org. Kur do të kombinoni të gjitha tre hapat, kërkimi në Google do të jetë:



Ja ku është në rezultatin e parë: ftesa për evenimentin.

FOS, me qendër në Kalgari (Calgary), shpesh etiketohet si një grup i mohimit të (ndryshimeve të) klimës dhe financohet pjesërisht nga sektori i naftës dhe gazit. Pra, si do të krijonim një kërkim për të gjetur më shumë informacion rreth organizatës dhe rrjetit të saj të mbështetësve dhe financuesve?

Hapi 1: Përfshijeni cakun

"Friends of Science" rezulton në shumë "goditje", andaj kyçeni po ashtu fjalën "Calgary."

Hapi 2: Përfshini "filetype" (llojin e dokumentit)

Kërkoni gjënë tjetër më të mirë për çdo dokument zyrtar, "filetype:pdf".

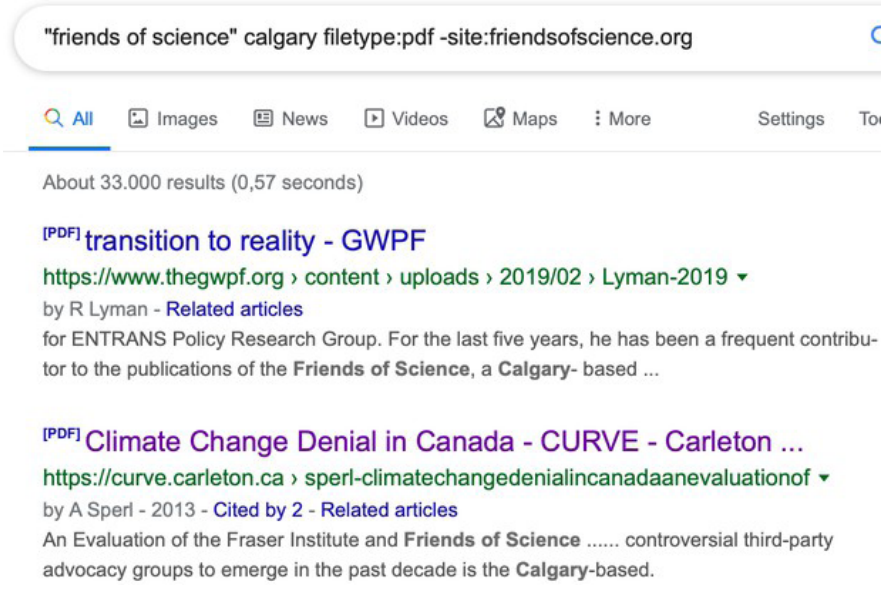
Hapi 3: Çkyçeni uebfaqen e cakut tuaj

Përjashtoni nga kërkimi uebfaqen e cakut tuaj Friendsofscience.org duke shtuar "-site:friendsofscience.org". Kjo ju ndihmon të gjeni informacione nga palët e jashtme.

Kërkimi i plotë është:

“friends of science” calgary filetype:pdf -site:friendsofscience.org

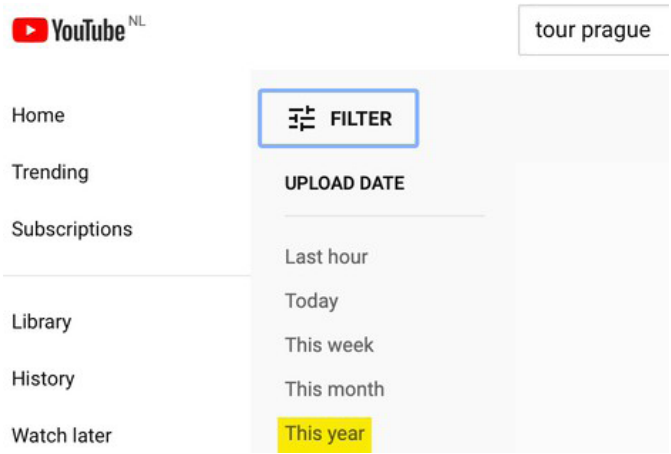
Për shkak se e keni kërkuar cakun tuaj në dokumente zyrtare, por jo nga uebfaqja e tij, do të gjeni disa përkrahës, por edhe ata që janë kritikë ndaj organizatës:



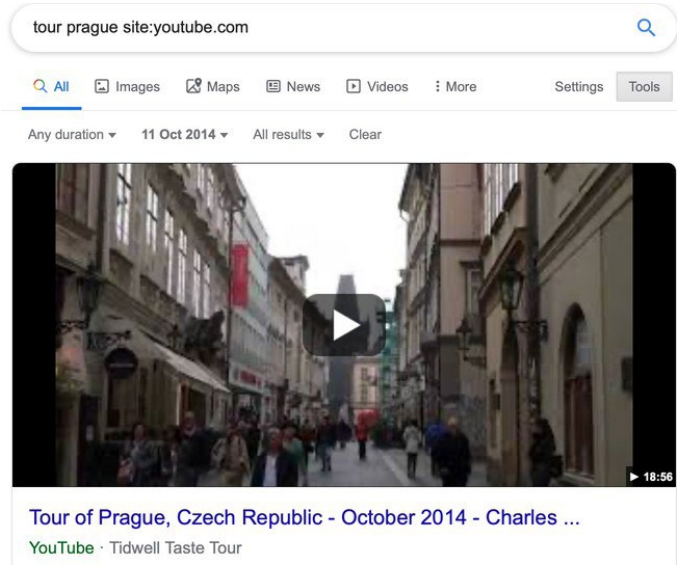
3. FILTRIMI I MEDIAVE SOCIALE PËR BURIME PRIMARE

YouTube

Mjeti i kërkimit i YouTube ka një problem: nuk do t’ju lejojë të filtroni videot që janë më të vjetra se një vit. Nëse dëshironi të gjeni një video të një turneu në Pragë nga 11 tetori 2014, kjo është pengesa në të cilën do të hasni:



Për ta zgjidhur këtë, futni manualisht datën e preferuar në një kërkim në Google.com duke përdorur menynë "Tools" në skajin e djathtë. Më pas zgjidhni "Çdo kohë" (Any time) dhe "Shtrirje me porosi" (Custom range). Kështu i marrim rezultatet që na duhen:

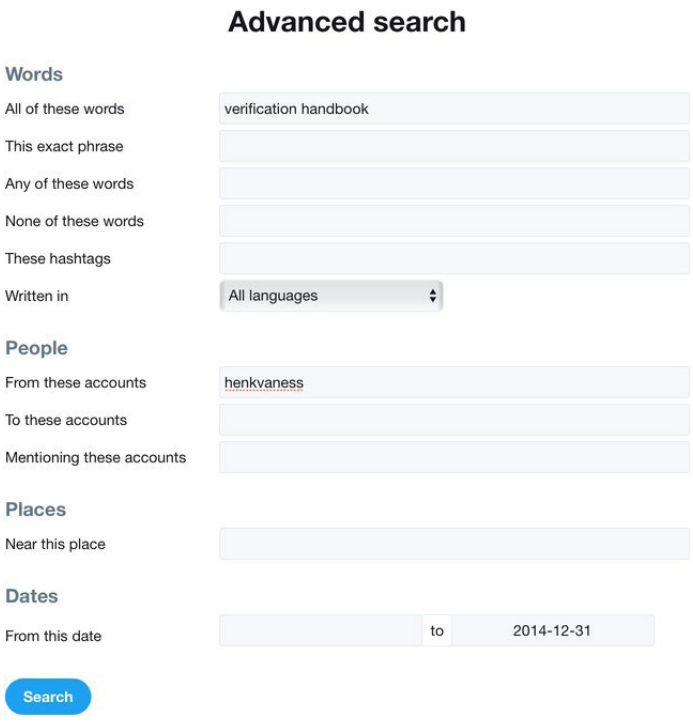


Twitter

Pavarësisht fuqisë së operatorit të kërkimit "site:", do të zhgënjeheni nëse e përdorni në Google për të provuar të kërkoni në Twitter. Për shembull, mund ta provojmë këtë kërkim për të gjetur kur kam postuar në Twitter për Doracakun e Verifikimit për herë të parë:

"verification handbook" site:twitter.com/henkvaness

Por, ju kthen vetëm një goditje nga ky shkrim. Motorët e përgjithshëm të kërkimit si Google shpesh e kanë të vështirë të japin rezultate cilësore nga triliona postime në Twitter, ose në platforma të mëdha si Facebook dhe Instagram. Përgjigja për Twitter është të përdoret funksionaliteti i Kërkimit të Avancuar të tij (Advanced Search) dhe të shtohen fjalë kyçe, emri i përdoruesit dhe periudha kohore, siç tregohet këtu:



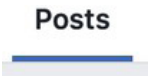
Mos harroni të klikoni në "Më e fundit" (Latest) në menynë në krye të faqes së rezultateve të kërkimit në mënyrë që të mund t'i shikoni rezultatet në rend të kundërt kronologjik. Zakonisht, Twitter i rendit rezultatet tuaja sipas asaj që ai i konsideron si tuite kryesore (top tweets).

Facebook

Përdorimi i "site:" në Facebook gjithashtu nuk është ideal, por mund të bëjmë që mjeti i tij i kërkimit të përshtatet me nevojat tona. Le të themi, për shembull, se dëshironi të shihni pos-time nga marsi 2019 në lidhje me tortën me luleshtrydhe nga njerëzit në Bruklin. Ndiqni këto hapa:

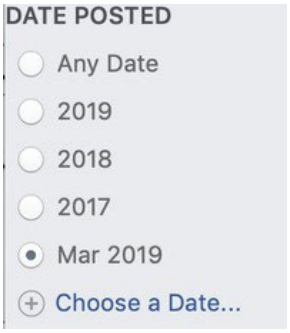
Hapi 1: Shtypeni kërkimin

Hapi 2: Klikoni në postime

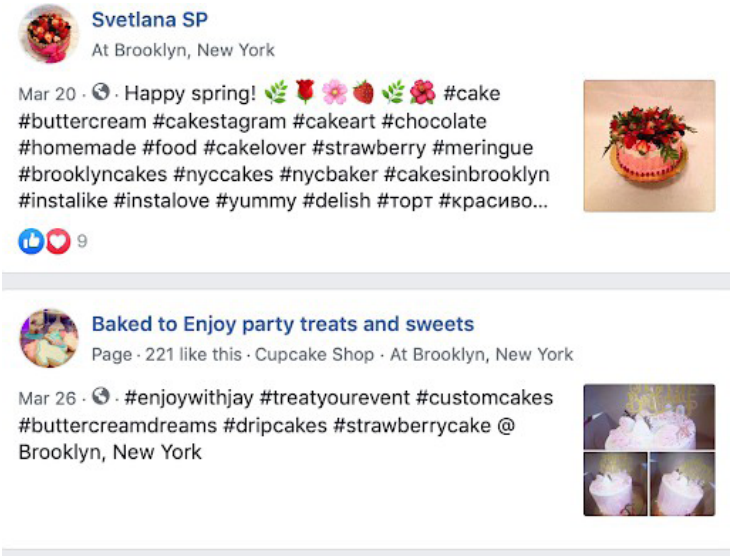


Hapi 3: Definoni lokacionin

Hapi 4: Zgjidhni një datë

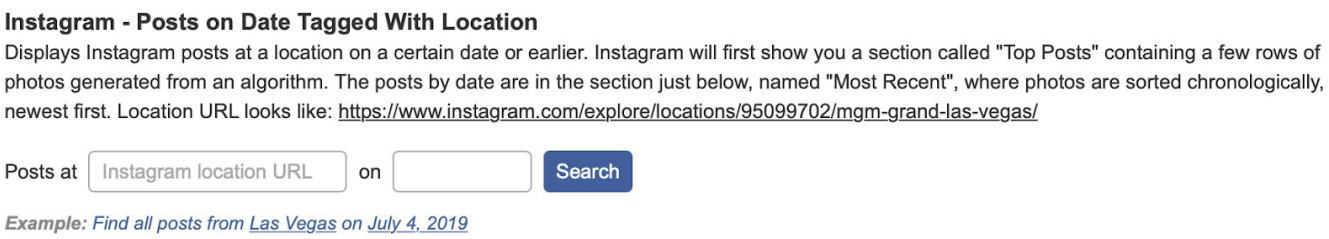


Dhe, ja ku e keni:



Instagram

Për të kërkuar në Instagram postime nga një datë specifike në një vend të caktuar, mund të shkoni në faqen time, whopostedwhat.com dhe të plotësoni kërkimin tuaj:



3. Njohja e botëve, kiborgëve dhe aktivitetit joautentik

Shkruajnë: Johana Uajlld , Sharlot Godart

Sharlot Godart *(Charlotte Godart) është hulumtuese dhe trajnere për Bellingcat. Para Bellingcat, ajo ishte e pjesë e Qendrës për të Drejtat e Njeriut në UC Berkli, ku punonte në Laboratorin Hulumtues të universitetit, dhe mësonte studentët se si të bëjnë hulumtime të burimeve të hapura (open-source) mbi konfliktet globale për entitetet ndërkombëtare humanitare.*

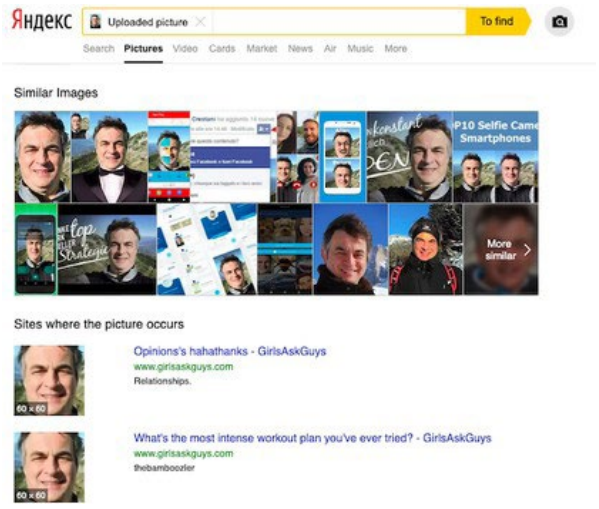
Johana Uajlld *(Johanna Wild) është një hulumtuese e burimeve të hapura në Bellingcat, ku fokusohet në teknologji dhe zhvillimin e mjeteve për hulumtime digjitale. Ajo ka përvojë në fushën e gazetarisë onlajn, e më parë ka punuar me gazetarë në rajone (post)konflikti. Një nga rolet e saj ishte t'i përkrahë gazetarët në Afrikën Lindore për të prodhuar transmetime për Zërin e Amerikës.*

Në fund të gushtit të vitit 2019, Bexhamin Strik (Benjamin Strick), një kontribues i Bellingcat-it dhe hulumtues i BBC Africa EYE, ka analizuar tuite që shpërndajnë hashtagjet #WestPapua dhe #FreeWestPapua, kur vuri re që llogaritë kishin një sjellje abnormale. Të gjitha këto llogari shpërndanin mesazhe pro qeverisë se Indonezisë, në periudhën kur konflikti në Papuan Perëndimore ishte duke marrë vëmendje ndërkombëtare, duke çuar në dhunë mes policisë së Indonezisë dhe protestuesve.

Llogaritë që i pa Striku shfaqnin ngjashmëri të shumta të çuditshme. Së shpejti, ai do të kuptonte se këta ishin indikatorë të hershëm të sjelljes së koordinuar joautentike. Mirëpo, së pari, ai filloi duke vënë re gjërat e vogla.

Për shembull, shumë nga llogaritë kishin fotografi të vjedhura profili. Merreni për shembull këtë llogari, që pretendoi të jetë e dikujt me emrin Marco:

Duke e përdorur mjetin e Yandex-it për kërkimin e kundërt të imazhit, Striku gjeti që fotografia e profilit të llogarisë ishte përdorur më parë në uebfaqe tjera me emra të ndryshëm. Asnjë nga këto llogari që përdornin fotografinë nuk ishin të personit real me emrin "Marko". Kjo dëshmoi që llogaritë ishin, së paku, mashtruese lidhur me identitetin e tyre të vërtetë.



Përtej mashtrimit për identitetin e tyre, Strik gjeti se llogaritë publikonin përmbajtje të ngjashme apo identike derisa shpesh e rituitonin njëra - tjetrën. Edhe më habitëse ishte se disa prej tyre shfaqnin një sinkronizim preciz në paternët kohorë të tuiteve të tyre. Për shembull, @Bellanowl dhe @Kevinma40204275 kryesisht publikonin tuitet në minutën e 7-të apo në minutën e 32-të të çfarëdo ore.

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

Është e pabesueshme që një njeri do të mund ta adoptonte një ritëm të tillë të tuiteve. Ky sinkronizim nëpër më tepër llogari të ndryshme, i kombinuar me fotot e tyre mashtruese, sugjeronte se llogaritë nuk ishin të lidhura me identitete reale dhe mund të ishin të automatizuara. Nga analizimi i paternëve (shablloneve) të llogarive të dyshimta si këto, Striku eventualisht konkludoi që llogaritë ishin pjesë e rrjetit të botëve pro-indonezian në Twitter që shpërndanin informacione keqorientuese dhe të njëanshme në lidhje me konfliktin në Papuan Perëndimore. (Mund të lexoni më shumë mbi këto llogari që ishin pjesë këtij rrjeti në kapitullin 11b rast studimi, "Hulumtimi i një Operacioni Informues në Papuan Perëndimore.")

Çfarë është një bot? Përgjigjja është më e komplikuar se ajo që e paramendoni

Rasti i Papuas Perëndimore është larg nga të qenët operacion informativ i vetëm që përdor bote sociale. Operacione tjera kanë qenë të bëra publike dhe kritikuara më gjerësisht, edhe pse në thelb ata përmbajnë ngjashmëri në mënyrën se si operojnë.

Boti është aplikacion softuerik që mund të performojë detyra të dhëna nga njerëzit në mënyrë automatike. Nëse një bot bën mirë apo keq tërësisht varet nga qëllimet e "pronarit" të tij.

Botëve që më së shumti u referohemi në debatet publike janë botë social, që janë aktiv në rrjetet sociale duke e përfshirë Facebookun, Twitterin, dhe LinkedIn-in. Në këto platforma, ata mund të përdoren për të shpërndarë mesazhe specifike ideologjike, shpesh me qëllim që ta bëjnë të duket sikur të jetë një përkrahje masive për ndonjë temë, person, përmbajtje apo hashtag të veçantë.

Botët në mediat sociale zakonisht bien në tre kategori kryesore: boti me orar (scheduled bot) , boti vëzhgues (watcher bot), dhe boti amplifikues (amplifier bot). Është e rëndësishme ta dimë se për cilin lloj të botëve jeni të interesuar, sepse çdo lloj e ka edhe qëllimin specifik. Me çdo qëllim vjen një gjuhë tjetër dhe një shabllon (patern) i komunikimit. Në kontekstin e dezinformatave, ne më së shumti jemi të interesuar ta shikojmë botin amplifikues.

Boti amplifikues ekziston që të bëjë saktësisht atë që përdoret në emërtimin e tij: të amplifikojë dhe shpërndajë përmbajtje, me synim për ta formësuar opinionin publik onlajn. Mund të përdoret edhe për t'i bërë individët dhe organizatat të duken që kanë një ndjekje më të madhe sesa që kanë realisht. Fuqia e tij vjen në numra. Një rrjet i botëve amplifikues mund të përpiqet të ndikojë mbi hashtagjet, të shpërndajë linqe apo përmbajtje vizuale, ose të grupohen për spam masiv, ose për të ngacmuar (sulmuar) ndonjë individ onlajn me qëllim për ta diskredituar ose për ta bërë të duket kontrovers apo "nën rrethim".

Duke punuar bashkë në numra të mëdha, botët amplifikues duken më legjitim, dhe prandaj ndihmojnë në formësimin e peizazhit të opinionit publik onlajn. Botët amplifikues që shpërndajnë dezinformata e bëjnë këtë kryesisht përmes fushatave të hashtagjeve ose duke shpërndarë lajme në forma të linqeve, videove, meme-ve, fotografive dhe llojeve tjera të përmbajtjes. Fushatat e hashtagjeve përfshijnë botë që në mënyrë të vazhdueshme, në koordinim, e rituitojnë të njëjtin hashtag, ose grup të hashtagjeve. Shpeshherë, qëllimi është ta mashtrojnë algoritmin e trendit të Twitterit duke e futur një hashtag specifik në listën e temave të trendit. Një shembull për këtë është "#Hillarysick" (Hilari e sëmurë), që është përhapur gjerë nga botët pasi Hillari Klinton u pengua në shtator të vitit 2016, shkurt pas zgjedhjeve presidenciale. (Po ashtu është e rëndësishme ta theksojmë që fushata e hashtagjeve nuk kërkon botë, dhe mund të jetë edhe më efektive pa ta. Shikojeni këtë hulumtim për "hashtag mullinjtë" me njerëz në Pakistan nga Dawn.)

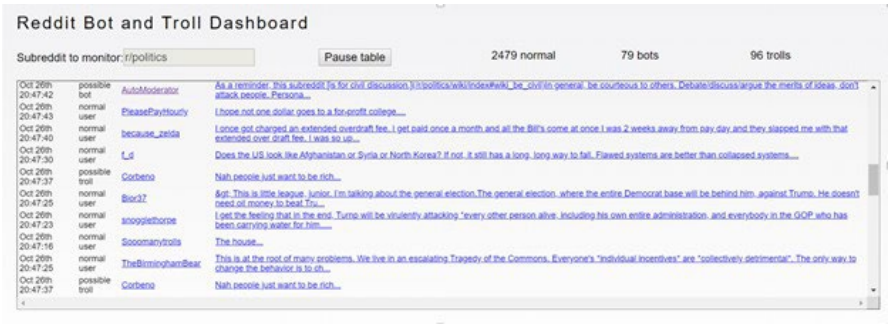
Blerja dhe krijimi i botëve është relativisht i lehtë. Faqe të panumërta do t'ju shesin ushtri botësh për disa qindra dollarë ose më pak. Por një rrjet i sofistikuar dhe gati-njerëzor është shumë më e vështirë për t'u krijuar dhe mirëmbajtur.

Si t'i njohim botët

Zhvilluesit e programeve (developerët) dhe hulumtuesit kanë krijuar mjete të ndryshme për të ndihmuar vlerësimin vallë një llogari mund të jetë e automatizuar. Këto mjete mund të jenë të dobishme në mbledhjen e informacioneve, mirëpo rezultati nga një mjet nuk është assesi definitiv dhe nuk duhet të përbëjë kurrë bazën e vetme për çdo raportim apo përfundim.

Njëra nga mjetet më të njohura është Botometer, i krijuar nga hulumtuesit në Universitetin Indiana. I bazuar në kritere të ndryshme, kalkulon një rezultat për atë se sa gjasa mund të ketë që një llogari e Twitterit apo përcjellësit e saj të jenë botë.

Për Reddit, Xhejson Skouronski (Jason Skowronski) ka krijuar një panel (dashboard) në kohë reale. Pasi ta vendosni për një subreddit të zgjedhur, përpiqet të vlerësojë nëse komentet janë bërë nga botët, trollët apo nga njerëzit.



Përderisa ka përjashtime, mjetet më të disponueshme publike për detektimin e botëve janë krijuar për Twitterin. Arsyeja është se shumë rrjete sociale - duke e përfshirë Facebookun - kufizojnë API-të (application programming interfaces) në mënyrë që e parandalon publikun nga analizimi dhe përdorimi i të dhënave të tyre për të krijuar kësi lloji mjetesh publike.

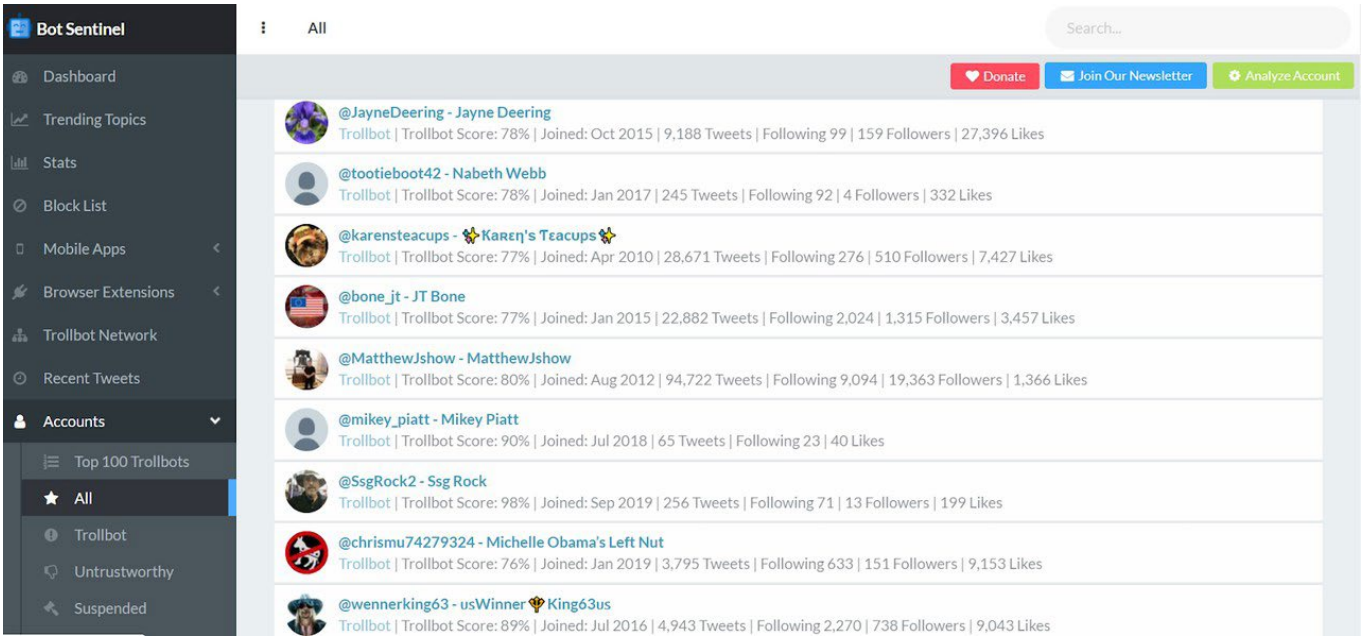
Siç u theksua më herët, mjetet e detektimit të botëve janë pikë e mirë e nisjes, por ato nuk duhet të jenë dëshmia juaj e vetme. Një arsye për shkallën e ndryshme të saktësisë së tyre është se thjesht nuk ka një listë universale të kritereve për njohjen e botëve me 100% siguri . Po ashtu, ekziston pajtueshmëri e ulët mbi klasifikimin e dikujt si bot. Studiuesit në Projektin e Propagandës Kompjuterike të Institutit të Internetit të Oksfordit klasifikojnë llogaritë që postojnë më shumë se 50 herë në ditë si llogari që kanë "automatizim të rëndë". Laboratori i Hulumtimit të Forenzikës Digjitale të Këshillit Atlantik i konsideron "72 tuite në ditë (një në dhjetë minuta për dymbëdhjetë orë me radhë) si të dyshimta dhe mbi 144 tuite në ditë si shumë të dyshimta".

Shpeshherë, mund të jetë sfidues përcaktimi vallë një fushatë e dezinformatave është kryer nga botët socialë ose njerëzit që janë të motivuar apo paguar të postojnë një numër të madh përmbajtjesh për një temë specifike. BBC, për shembull, ka gjetur që llogaritë që kanë postuar mesazhe të ngjashme në Facebook duke amplifikuar përmbajtje të favorshme për Boris Xhonsonin në nëntor të vitit 2019 që kanë qenë të menaxhuara nga njerëz që kanë aktruar sikur janë botë socialë.

Po ashtu, mund të hasni edhe në kiborgë, llogari të mediave sociale që janë pjesërisht të automatizuara e pjesërisht të menaxhuara nga njerëz, që shfaqin një kombinim të sjelljes natyrale dhe joautentike. Gazetarët duhet t'iu shmangen emërtimeve të llogarive të dyshimta si botë pa dëshmi dhe analizë të duhur, sepse akuza e gabueshme mund t'ua ulë kredibilitetin.

Një mënyrë për t'u marrë me këto lloje të ndryshme të botëve, kiborgëve dhe llogarive hiper-aktive të njerëzve është që të fokusoni hulumtimin tuaj në monitorimin e të gjitha sjelljeve jo-autentike apo të ngjashme me të botëve, në vend që të përpiqeni të identifikoni vetëm një lloj të llogarive të dyshimta.

Për shembull, Bot Sentinel ofron data-bazë të qasshme publik që përmban llogari amerikane të Twitterit që shfaqin sjellje të dyshimtë. Krijuesit e tyre kanë zgjedhur që të mbledhin "llogari që vazhdimisht i kanë shkelur rregullat e Twitterit" në vend që të kërkojnë specifikisht botët socialë.



Hapat për hulumtimin e sjelljes joautentike

Në përgjithësi, sugjerojmë qasjen në vijim për identifikimin e sjelljes joautentike dhe potencialisht të automatizuar në rrjetet sociale:

1. Kontrolloni në mënyrë manuale llogaritë për sjellje të dyshimtë.
2. Kombinoni këtë me përdorimin e mjeteve apo me analizë më teknike të rrjeteve.
3. Hulumtoni aktivitetin e tyre, përmbajtjen dhe rrjetin e llogarive tjera me të cilat ndërvepro-jnë. Kombinoni këtë me teknikat tradicionale hulumtuese, si përpjekja për t'i kontaktuar ata apo njerëzit që pretendojnë se i njohin.
4. Këshillohuni me ekspertë të jashtëm që janë specialistë mbi botët dhe aktivitetin joautentik.

Që të mësojmë se si t'i vlerësojmë manualisht llogaritë e dyshimta, është e rëndësishme t'i kuptojmë shenjat tipike paralajmëruese për llogari të automatizuara në Twitter, ose në rrjete tjera sociale.

Çdo bot i medias sociale ka nevojë për një identitet. Krijuesit e botëve duan t'i bëjnë llogaritë të paraqiten sa më të besueshme që mundet, por merr kohë për t'i rregulluar dhe mirëmbajtur profilet me pamje të besueshme, veçanërisht nëse qëllimi është të udhëhiqet një rrjet i madh i botëve. Sa më shumë llogari që ka dikush, aq më shumë kohë merr për t'i krijuar dhe me-naxhuar në mënyrë që të duken autentike. Këtu është pjesa ku këto llogari bëjnë gabime. Në shumë raste, krijuesit e tyre e bëjnë minimumin për të krijuar një profil, dhe një hulumtues i mirë mund ta detektojë këtë.

Ja disa gjëra që duhet shikuar:

Nuk ka fotografi të vërtetë të profilit

Një fotografi e vjedhur (siç shihet në hulumtimin e Papuas Perëndimore të Bexhamin Strikut) ose mungesë e fotografisë së profilit, mund të jetë indikator i joautenticitetit. Pasi që krijuesit e botëve duan të krijojnë shumë llogari përnjëherësh, ata duhet të gjejnë një koleksion të fotografive dhe shpesh i kopjojnë ato nga uebfaqet tjera. Sidoqoftë, kjo përgjatë bërjes krijon mospërputhje. Për shembull, një llogari me foto profili të një mashkulli por me emër të përdoruesit që nënkupton se llogarinë e posedon një femër mund të jetë sinjal se diçka nuk është në rregull. Për ta zgjidhur këtë çështje, shumë krijues të botëve zgjedhin karakterë vizatimorë apo kafshë si foto të profilit, por përsëri kjo taktikë bëhet edhe një patern që përdoret për detektimin e llogarive joautentike apo botëve.

Emra të përdoruesve të krijuar automatikisht

Në vijim, kërkoni emrat dhe emrat e përdoruesve. Çdo dorezë Twitteri është unike, që domethënë se emrin e përdoruesit që e dëshiron shpeshherë është veçmë i zënë. Kjo është një pengesë për njerëz të zakonshëm, por bëhet një sfidë e vërtetë kur përpiqesh ti krijosh 50, 500 ose 5000 llogari për një periudhë të shkurtë kohore.

Krijuesit e botëve shpesh vendosin një strategji që t'u ndihmojë të gjejnë më lehtë emra përdoruesish të papërdorur. Skripta me kriteret sikurse këto në vijim përdoren për të krijuar automatikisht emra përdoruesish:

Emër përdoruesi i pasuar me një numër 4 shifror	12 karaktere të rastësishme në gjatësi që mund të përbëhen nga (a-z A-Z dhe 0-9)	Çfarëdo emër i përveçëm i pasuar nga një numër i rastësishëm tetëshifror, që tregon se është përdorur emri i paracaktuar i përdoruesit i krijuar nga Twitteri.
superman_1230 superman_2313 superman„9832 superman_3934 superman_4920	vPltfllZoPGl dNi29j2utANQ YQBrodhbPC84 TUq3R6GBWYyA XI87NreGshx8	Neil03121977 Sarah92839820 | Claire02938593 John09340293 Stephen837492 84

Kur e vini re që llogari të ndryshme me doreza të Twitterit përbëjnë të njëjtin numër të karaktereve dhe numrave, mund të kërkoni manualisht për më shumë llogari me atë model (patern) në secilën listë të ndjekësve të llogarisë që potencialisht ta identifikoni një rrjet.

Në këtë shembull, llogaritë që kanë diçka të përbashkët: të gjitha ato janë krijuar në shtator të

vitit 2019. Kur kombinohet me sinjale tjera, kjo mund të jetë një indikator që llogaritë janë bërë në të njëjtën kohë nga i njëjti person.

Aktiviteti i llogarisë nuk përshtatet me moshën

Duhet të bëheni edhe më dyshues nëse një llogari e re veçmë ka një numër relativisht të madh të ndjekësve ose nëse ka publikuar një numër të madh të tuiteve brenda një kohe të shkurtë. E njëjta vlen edhe nëse një llogari e vjetër ka shumë pak ndjekës edhe pse është shumë aktive.

Nëse bini ndesh me llogari të tillë, analizojeni më thellë aktivitetin e tuiteve të llogarisë. Merreni numrin e tuiteve të vendosura në krye të faqes dhe pjesëtojeni këtë me numrin e ditëve qëkur llogaria ka qenë aktive. Për shembull, merreni një llogari që ka 3,489 tuite gjer më 11 nëntor 2019, e është krijuar më 15 gusht 2019. Pjesëtojeni me 89 (ditët që ka qenë aktive), dhe do të fitoni 39.2 tuite në ditë.

Duke parë tuitet e bëra përgjatë ekzistimit së llogarisë, a duket numri shumë i lartë, joreal dhe i pamundur për t'u mirëmbajtur?

Paterne (modele) të dyshimta të tuiteve

Një element tjetër për t'u ekzaminuar është ritmi i tuiteve. Njerëzit shfaqin preferenca të vogla për ditët dhe kohën kur ata zakonisht publikojnë tuite, por është e pazakonshme që një person të publikojë vazhdueshëm vetëm të hënën, të martën, dhe të mërkurën dhe të jetë tërësisht i heshtur përgjatë ditëve tjera të javës për një periudhë të gjatë.

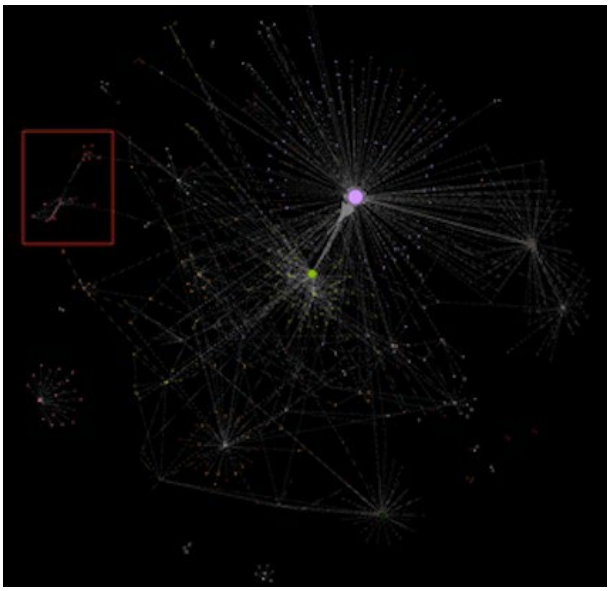
Nëse dëshironi t'i shihni këto modele (paterne) të vizualizuara për një llogari specifike, shikoni mjetin për analizë të llogarive të krijuar nga Lluka Hamer (Luca Hammer):

\

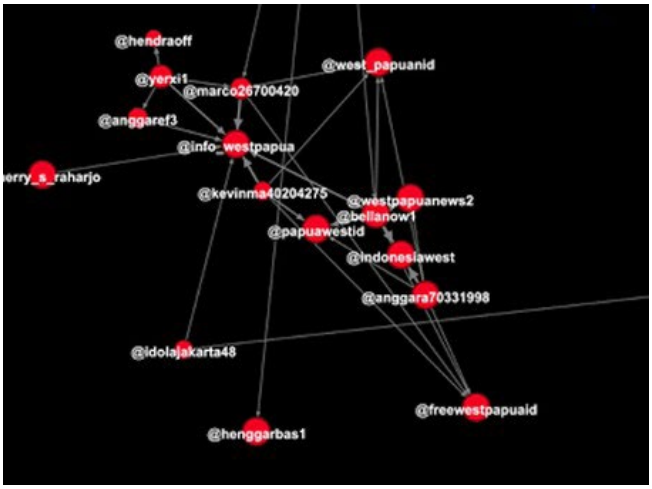
Vizualizimi si pjesë e hulumtimit tuaj

Për ta kuptuar më mirë aktivitetin e të gjithë rrjetit të botëve, mund ta përdorni një platformë vizualizuese si Gephi. Kontribuesi i Bellingcat-it, Benjamin Striku e përdori këtë mjet për të analizuar lidhjen mes llogarive të Twitterit që i takonin një rrjeti të botëve pro-Indonezian.

Duke shikuar në përfaqësimin vizual të lidhjeve ndërmjet një numri të madh të llogarive të Twitterit, ai vuri re që struktura në anën e majtë të fotografisë (me të kuqe) binte në sy.



Duke e zmadhuar (zumuar) atë zonë, ai mund të shihte se cilat llogari të Twitterit ishin pjesë e kësaj strukture specifike.



Çdo rreth i kuq përfaqëson një llogari Twitteri, kurse vijat janë marrëdhëniet mes tyre. Zakonisht, llogaritë e vogla janë të renditura përreth një rrethit më të madh në mes, që do të thotë se ato të gjitha komunikojnë me llogarinë ndikuese. Llogaritë në strukturën sipër, sidoqoftë, nuk komunikojnë në atë mënyrë me njëra-tjetrën. Kjo e çoi Strikun t'i analizojë ato sjellje abnormale të llogarive.

E ardhmja e botëve social: A mund t'i mbi-mashtrojmë ata?

Teknologjia prapa botëve social është bërë edhe më e avancuar në vitet e fundit, duke lejuar aplikacionet e vogla softuerike të bëhen më të afta në simulimin e sjelljes njerëzore. Jemi duke ardhur në një pikë ku njerëzit janë duke parashikuar se përdoruesit artificialë mund të angazhohen në komunikime të sofistikuara onlajn në mënyrë që bashkëbiseduesit e tyre –njerëz nuk do të kuptojnë se në të vërtetë po bëjnë një bisedë të gjatë me një bot.

Megjithatë, deri më tani nuk ka asnjë provë që botët socialë të nivelit të lartë të fuqizuar nga makinat inteligjente ekzistojnë ose janë duke u vënë në përdorim. Tani për tani, duket se shumë fushata dezinformuese aktualisht po marrin ende mbështetje nga botët amplifikues që janë më pak kompleks.

"Nuk mendoj që ka aq shumë botë socialë të sofistikuar që janë në gjendje të bëjnë një bisedë reale me njerëz dhe t'i bindin për pozicione politike të caktuara", tha Dr. Ole Piitz, hulumtues për projektin "Botë të paanshëm që ndërtojnë ura" në Universitetin Bielefeld në Gjermani.

Sipas tij, mënyra më e mirë për ta ndihmuar publikun për t'i njohur sjelljet joautentike në rrjetet sociale është përdorimi i metodës së detektimit që kategorizon dhe peshon të gjithë faktorët që e bëjnë një llogari të dyshimtë. Si një shembull, thotë ai, "Kjo llogari përdor skriptë për të rituituar lajme, automatikisht i ndjek të tjerët, dhe kjo kurrë nuk përdor modele (paterne) të të folurit që i përdorin zakonisht njerëzit."

Tani për tani, një analizë metodike e sjelljes së llogarisë, përmbajtjes, ndërveprimit dhe modeleve (paternëve) mbetet si qasje më e mirë për identifikimin e sjelljes joautentike.

Në kapitullin tonë të rastit të studimit, ofrojmë një shpjegim më të thellë dhe më teknik se si i kemi analizuar faktorët e ndryshëm në një rrjet të dyshuar në Twitter në lidhje me protestat në Hong Kong.

3a. Rast Studimi:
Gjetja e provave për aktivitet të automatizuar në Twitter gjatë protestave në Hong Kong

Shkruajnë: Sharlot Godart, Johana Uajlld

Sharlot Godart *(Charlotte Godart) është hulumtuese dhe trajnere për Bellingcat. Para Bellingcat, ajo ishte e pjesë e Qendrës për të Drejtat e Njeriut në UC Berkli, ku punonte në Laboratorin Hulumtues të universitetit, dhe mësonte studentët se si të bëjnë hulumtime të burimeve të hapura (open-source) mbi konfliktet globale për entitetet ndërkombëtare humanitare.*

Johana Uajlld *(Johanna Wild) është një hulumtuese e burimeve të hapura në Bellingcat, ku fokusohet në teknologji dhe zhvillimin e mjeteve për hulumtime digjitale. Ajo ka përvojë në fushën e gazetarisë onlajn, e më parë ka punuar me gazetarë në rajone (post)konflikti. Një nga rolet e saj ishte t'i përkrahë gazetarët në Afrikën Lindore për të prodhuar transmetime për Zërin e Amerikës.*

Në gusht të vitit 2019, Twitteri shpalli fshirjen e mijëra llogarive të Twitterit për të cilat tha se kanë ndihmuar në shpërndarjen e dezinformatave në lidhje me protestat në Hong Kong dhe kanë qenë pjesë e "operacionit të koordinuar të përkrahur nga shteti". Së shpejti, Facebooku dhe YouTube dolën me kumtesa duke thënë se edhe ata kanë mënjanuar llogari që janë përshirë në sjellje joautentike të koordinuar në lidhje me protestat.

Përkundër Facebookut dhe YouTube-it, Twitteri nxori një listë të llogarive që i ka mënjanuar, duke ofruar një mundësi për ta hulumtuar më tej aktivitetin. Me një pjesëmarrës të një punëtorie të Bellingcat-it, ekipi ynë vendosi që t'i hulumtojë përmbajtjet e mbetura të Twitterit në lidhje me protestat në Hong Kong për t'u përpjekur që të identifikojë shenjat e sjelljes joautentike të koordinuar.

Gjetja e aktivitetit të dyshimtë

Filluam duke kërkuar për hashtagje relevante në lidhje me protestat. Një fjalë kyçe e thjeshtë për "Hong Kong Riots" solli shumë tuite, mes tyre disa që përmbanin më shumë hashtagje.

Deshëm të fokusohemi në llogaritë dhe përmbajtjet pro Kinës, pasi që këto ishin tato për të cilat Twitter veçmë kishte gjetur se janë përfshirë në aktivitet joautentik. Provuam formulime të fjalëve kyçe si për shembull ky:

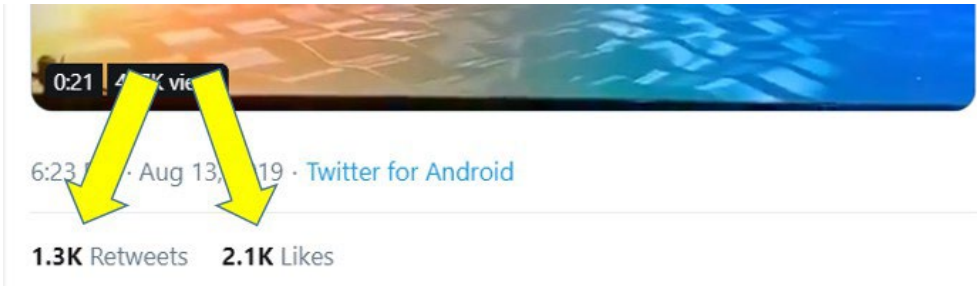
"Shame on Hong Kong" -police –government ("Turp për Hong Kongun" -policinë –qeverinë e)

Ky kërkim jep rezultate që përmbajnë frazën "Shame on Hong Kong" por jo fjalët policia ose qeveria. Qëllimi ishte të filtrohen tuitet si "shame on Hong Kong police"(turp për policinë e Hong Kongut) dhe të mbahen tuitet si "shame on Hong kong protesters" (turp për protestuesit e Hong Kongut). Tjerat terme të kërkuara ishin "Hong Kong roaches" (kacabutë e Hong Kongut) dhe "Hong Kong mobs" (turmat e Hong Kongut), që ishin përshkrues të zakonshëm të protestuesve nga llogaritë pro-kineze të Twitterit.

Pas përdorimit të këtyre dhe disa termeve tjera të kërkimit, i ekzaminuam tuitet e fundit në lidhje me Hong Kongun që morën shumë rituite dhe pëlqime. Mund t'i filtroni sipas angazhimit (engagement) thjesht duke shtuar "min_retweets:500" ose "min_faves:500" në kërkimin tuaj. Kjo do t'ju nxjerrë vetëm tuite që kanë të paktën 500 rituite dhe pëlqime.

Pastaj, i shikuam llogaritë e Twitterit që kishin ndërvepruar me ato tuite. Për shembull, aty ishte një tuit nga një përdorues i verifikuar Hu Xijin, kryeredaktor i botimeve kineze dhe angleze të Global Times, një media shtetërore kineze:

Ne klikuam në hiperlinqet për "rituite" dhe "pëlqime" pranë çdo numrit të angazhimit për ta shfaqur listën e llogarive që kanë kryer veprimin relevant.

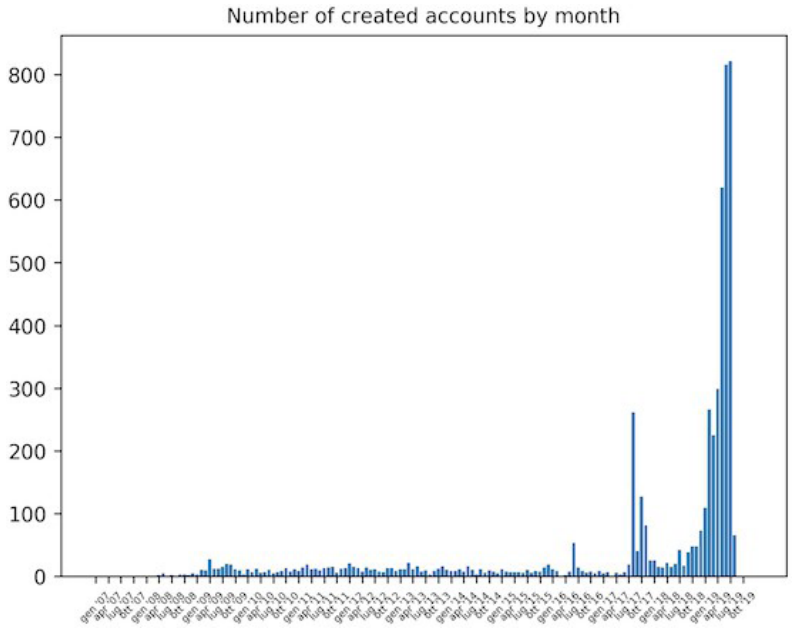


Hipoteza jonë ishte se llogaritë joautentike pro-kineze do të kishin amplifikuar tuite nga personeli i njohur i medias shtetërore kineze. Në këtë rast, shumë emra përdoruesish binin në sy, sepse kishin numër tetëshifror pas emrit, që ishte tregues se përdoruesi ka pranuar emër të paracaktuar të gjeneruar nga Twitteri kur ishte regjistruar. Kjo siguroi hulumtim të mëtejshëm në sjelljen dhe karakteristikat e tyre.

Teksa i kontrolluam këto llogari, e pamë se ato kishin një numër të vogël të ndjekësve, përcillnin vetëm disa llogari, nuk dispononin me biografi, rituitonin tuitet e njerëzve tjerë e vetë nuk prodhonin gati se asnjë, dhe gati ekskluzivisht promovonin përmbajtje që ishte në kundërshtim me protestat.

Po ashtu, vumë re që datat e krijimit të këtyre llogarive ishin shumë të freskëta, rreth gushtit të vitit 2019. Pasi Twitteri nxori një listë të llogarive pro kineze që i kishte fshirë, ne kishim mundësi t'i kontrollonim datat e krijimit të këtyre llogarive dhe të shihnim nëse shfaqnin një trend të ngjashëm.

Me ndihmën e Luigji Gubellos (Luigi Gubello), kodues i angazhuar në një komunitet të burimeve të hapura (open-source) onlajn, përdorëm një skriptë të thjeshtë të Python-it (mund ta gjeni kodin në GitHub-in e tij, po ashtu edhe më shumë informacione në lidhje me të këtu) për t'i identifikuar shablonët (paternët) në të dhënat. Grafiku i mëposhtëm tregon se të gjitha llogaritë e fshira ishin krijuar në muajt e fundit, gjë që lidhet me karakteristikat e një grupi të llogarive aktive që ishim duke e hulumtuar.



Automatizimi i procesit

Tani që e identifikuam një mostër të tuiteve që shfaqnin sjellje dhe karakteristika të dyshimta, deshëm që ta kryejmë një analizë shumë më të madhe. Kjo kërkonte njëfarë automatizimi. Një pjesëmarrës në punëtorinë e Bellingcat-it kishte përvojë në zhvillim të softuerëve, kështu që ai e shkroi një pjesë të vogël kodi për JavaScript – shprehjen e zakonshme (\w+\d{8}) - për të performuar dy funksione: të ekstraktojë emrat e përdoruesve të llogarive që kanë rituituar apo pëlqyer një tuit specifik, e pastaj të filtrojë shpejtë listën e emrave të përdoruesve duke u fokusuar vetëm në emrat e përdoruesve që i përshtateshin këtij paterni (shablloni). Paternin që filtroi ai ishte emër i pasuar me numër tetëshifror.

Duke e ngarkuar këtë skriptë në Chrome developer tools console (konsolën e veglave të developerëve të Chrom-it), që ofron mjete të zhvillimit të uebfaqeve drejtpërdrejtë në kërkues, ai do të funksiononte në sfond sa herë që ai klikonte në hiperlinkun për "rituit" apo "pëlqim" për një tuit specifik. Pastaj, do të kthente rezultatet që theksonin emrat e përdoruesve që i përshtaten paternit (shablonit). Shkoni këtu për të parë se si duket kjo.

Tani mund ta përdornim skriptën e tij për t'i kontrolluar llogaritë që ndërveprojnë me tuite tjera të pro - kineze të njohura. Në mes të protestave së Hong Kongut, aktorja kinezo-amerikane Liu Yifei shpërndau një post të Weibo-së në përkrahje të policisë, që çoi disa njerëz në rrjete sociale të bënin thirrje për bojkotim të filmit të saj të ri, "Mulan". Mirëpo, vumë re se shumë llogari Twitteri e përkrahën aktoren dhe filmin e saj duke e përdorur hashtagun #përkraheni Mulanin - #SupportMulan (edhe CNN-i raportoi mbi këtë). Vendosëm ta përdornim skriptën për t'i kontrolluar përdoruesit që e kishin rituituar apo pëlqyer tuitet pro Mulanit.

I mblodhëm emrat e llogarive që përshtateshin me paternin tonë dhe i identifikuam datat e tyre të krijimit. Kjo zbuloi se shumica e llogarive ishin krijuar më 16 gusht.

https://twitter.com/monicaG62882882	created: 16 August, 20.07h
https://t	Број на креирани сметки по месец 9h
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

I mblodhëm datat dhe kohën ekzakte të krijimit të llogarive thjesht duke mbajtur kursorin sipër (hovering over) informacionit mbi bashkëngjitjen e profilit ("joined"), siç shfaqet më poshtë:

Me një grup të llogarive para nesh, filluam analizë manuale të përmbajtjeve që kishin shpërndarë. U bë e qartë shumë shpejtë se të gjitha llogaritë në listën tonë kishin tuituar në favor të Yifeit dhe kundër protestuesve të Hong Kongut.

Shumë nga llogaritë në listën tonë u bënë joaktive pas 17 apo 18 gushtit, gjë që përsëri tregoi një element të koordinimit. Nuk e dimë saktë se pse të gjithë u pasivizuan, por është e mundur që Twitteri të ketë kërkuar hapa shtesë të verifikimit nga krijuesit që të kyçen, kurse ata e kishin të pamundur t'i përmbushin. Një opsion tjetër është që ata thjesht ndaluan së tuituari sepse krijuesit e llogarive nuk kanë dashur të ngritin dyshime të mëtejme pasi Twitteri filloi t'i suspendojë llogaritë pro Kinës.

Mirëpo, pas disa muajve, vumë se disa nga llogaritë ishin përsëri aktive. Këtë herë ata shpërndanë porosi pozitive për Yifein dhe filmin e saj Mulanin.

Po ashtu, gjetëm "pro – Mulan" llogari me paternë tjerë të emrave të përdoruesve apo data krijimi që shpërndanin vazhdimisht porosi në favor të Yifeit. E bëmë këtë herë duke kërkuar për tuite që përfshinin hashtagje sikur #SupportMulan ose #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

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?

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 😘😘😘

Si duket llogaritë e ndërruan strategjinë e tyre nga të kritikuarit e protestuesve të Hong Kongut në promovimin e aktores dhe filmit të saj, me siguri që ta shmangnin bllokimin nga Twitteri.

Ky rast i studimit tregon se si është e mundur të kombinohen teknikat manuale dhe të automatizuara për të zbuluar shpejtë rrjetet e llogarive të dyshimta në Twitter. Po ashtu, ai ilustron se si është e dobishme të kërkoni llogari të tjera dhe aktivitete edhe pasi platforma të lajmërojë për heqjen e llogarive.

Këtu, kishim mundësinë të përdorim disa teknika të thjeshta kërkimi dhe detaje të llogarive për të identifikuar një grup më të madh të llogarive që shfaqën shenja të përfshirjes në aktivitet joautentik të koordinuar.

4. Monitorimi i mashtrimeve dhe operacioneve të informacionit gjatë lajmeve të fundit

Shkruan: Xhejn Litvinenko

Xhejn Litvinenko *(Jane Lytvynenko) është reportere seniore në BuzzFeed News, ku fokusohet në dezinformatat, sigurinë kibernetike dhe hulumtimet në internet. Ajo ka zbuluar fushata manipulimi në media sociale, mashtrues të kriptomonedhave dhe aktorë të këqij të motivuar financiarisht që përhapin dezinformata. Puna e saj sjell gjithashtu kontroll të qasshëm të verifikimit të fakteve për audienca të gjera gjatë kohërave të krizës. Xhejn është nga Kievi, Ukraina dhe aktualisht banon në Toronto, Kanada.*

Kur dalin lajmet e fundit (breaking news), mund të kalojnë orë apo edhe ditë derisa gazetarët dhe zyrtarët të jenë plotësisht në gjendje të kuptojnë një situatë. Ndërsa provat dhe detajet e hershme fillojnë të qarkullojnë në rrjetet sociale dhe platformat e tjera në internet, mund të shfaqen aktorë të këqij për të mbjellur ndarje ose mosbesim, ose për të fituar shpejt vëmendjen e një konsumatori të shqetësuar të lajmeve. Të njëjtët konsumatorë me qëllime të mira dhe burime të tjera gjithashtu mund të përhapin pa dashje informacion të rremë ose keqorientues. Përzierja e emocioneve të shtuara dhe rrjedhja e ngadaltë e lajmeve në minutat dhe orët e para të një ngjarjeje e bën të nevojshme që gazetarët të jenë të pajisur për të monitoruar, verifikuar dhe - kur është e nevojshme - për të përgënjeshtruar lajmet e fundit. Një tuit, imazh, llogari në media sociale apo artikull i rremë kërkon vetëm disa minuta për t'u krijuar, ndërsa informacioni i vërtetë ka vështirësi që të mbajë hapin.

Kyçe për monitorimin dhe zbulimin gjatë lajmeve të fundit është të vendosësh një themel të fortë përpara se të ndodhë. Kjo do të thotë të kesh një bazë solide në aftësitë themelore të verifikimit, si ato të përshkruara në Doracakun e parë të Verifikimit, të kuptosh se si të monitorosh rrjetet dhe platformat sociale dhe të dish se si të përgjigjesh nëse ju ose kolegët tuaj bëheni objektiv i aktorëve të këqij. Gazetarët nuk duhet kurrë të neglizhojnë sigurinë në internet.

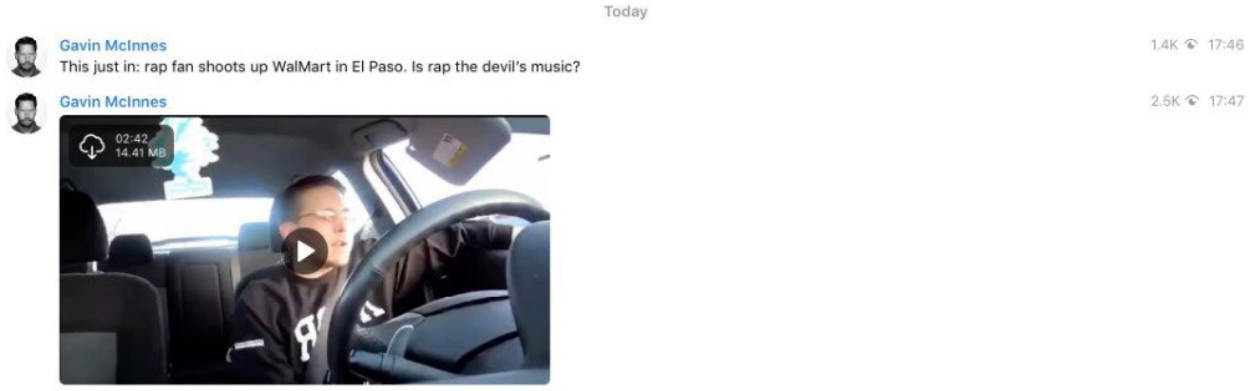
Kur dalin lajmet e fundit, hapi i parë është identifikimi i komuniteteve kryesore të prekura. Gjatë të shtënave në vitin 2018 në shkollën e mesme në Parkland, Florida, gazetarët hulumtuan hartën e Snapchat-it për videot e asaj që po u ndodhte studentëve të bllokuar brenda klasave. Për dallim nga ky rast, gjatë uraganit Irma në 2017, ishte thelbësore të fokusohesh në Facebook, ku të prekurit u përpoqën të gjenin informacion. Të kuptuarit se si funksionon çdo rrjet social dhe si ndërthuret me një ngjarje të caktuar është thelbësore.

Ky kapitull do të fokusohet në mjetet që një reporter mund të përdorë për monitorimin dhe përgënjeshtrimin e lajmeve të fundit. Jo çdo mjet do të jetë i përshtatshëm për çdo situatë, dhe të kuptuarit se kush është prekur mund t'ju ndihmojë të dini se në cilat vende duhet të fokusoheni më shumë.

Tri gjëra për të kërkuar

Përderisa platformat edhe raportuesit punojnë shumë për t'i luftuar dezinformatat, taktikat e aktorëve të këqij për ta shmangur detektimin kanë evoluar. Por përsëri, shfaqen disa shablone (paterne) të vazhdueshme përmbajtjesh dhe sjelljesh në mënyrë të përsëritur.

1. Imazh i ndryshuar ose jashtë kontekstit. Imazhi famëkeq i një peshkaqeni që notonte në autostradë të vërshuar ka qarkulluar shumë dhe vazhdimisht, për t'i mashtruar njerëzit me vite. (Gjithashtu, ishte edhe subjekt i rastit të studimit në Doracakun e parë.) Fotografitë dhe videot që janë përgënjeshtruar më parë janë ato që verifikuesit e fakteve dhe zbuluesit i quajnë mash-trime zombi dhe janë të rëndësishme për t'u përcjellë. Imazhet shpërndahen shumë më shpejtë në platforma sesa teksti, prandaj fokusimi mbi to shpeshherë është frytdhënës.



Gjatë të shtënave në El Paso në një Walmart në 2019, personazhet e së djathtës ekstreme u përpoqën të keqinterpretonin një video të vjetër në YouTube që nuk kishte lidhje me të dyshuarin.

2. Viktima apo autorë të rremë të krimeve. Gjatë gjuajtjeve në zyrat e YouTube, rrjetet sociale ishin të mbushura me pretendime të rreme për të dyshuarit. Gjatë zgjedhjeve afatmesme (midterm elections) në ShBA në vitin 2018, thashetheme të rreme për votat e hedhura nga emigrantë ilegal u përhapën nga presidenti i ShBA. Autorët e rremë të krimeve shfaqen gjatë shumicës së ngjarjeve të mëdha të lajmeve të fundit.

Gjatë të shtënave në Parkland 2018, një llogari e rreme e Bill O'Reilly u përpoq të përhapte një emër të rremë për të dyshuarin.

3. Ngacmimi (maltretimi) dhe brigadimi. Ndonëse nuk konsiderohet strikt si dezinformim, aktorët e këqij zakonisht përpiqen të ngacmojnë njerëzit e përfshirë në një ngjarje lajmesh si një mënyrë për t'i heshtur. Është gjithashtu një shenjë se një grup njerëzish po i kushtojnë vëmendje një ngjarjeje dhe mund të provojnë taktika të ndryshme gjatë rrugëtimit. Brigadimi (brigading) është kur një grup njerëzish punojnë së bashku për të krijuar përshtypjen e një jehone angazhimi ose reagimi, duke bërë gjëra të tilla si përmbajtje votimi "lart" ose "poshtë" ose duke vërshuar një përdorues me komente.

Pas një debati të liderëve të Demokratëve në vitin 2019, llogari anonime përhapën të njëjtin mesazh për garën e Kamala Harris.

Praktikat më të mira për arkivim dhe publikim

Përpara se të kërkoni mashtrime (hoax-es), hapeni një folder (dosje) për dokumentet tuaja dhe filloni një tabelë për atë që gjeni. Bëni menjëherë skrinshot të çdo mashtrimi dhe përmbajtjeje relevante që zbuloni dhe arkivojeni faqen. (Ekstensioni i shfletuesit të uebit Archive.org është një mjet falas, i shpejtë dhe efektiv për arkivimin e përmbajtjes). Sigurohuni që të regjistroni URL-të origjinale dhe të arkivuara të përmbajtjes në tabelën tuaj. Kjo ju mundëson të ktheheni tek ajo që keni gjetur dhe të kërkoni paterne (shabllone) pasi të "bjerë pluhuri".

Për të shmangur që të ndihmoni përhapjen e faqeve të lidhura me dezinformata ose misin-formata (informata të gabueshme), sigurohuni që, në vend të origjinalit, të lidhni URL-në e arkivuar në çdo artikull ose postim të mediave sociale,. Është gjithashtu një praktikë e mirë të vendosni vulë apo shenjë (watermark) në imazhet tuaja me një etiketë të qartë si "E rreme" ose "Keqorientuese" për t'u siguruar se ato do të shpërndahen dhe indeksohen me kontekstin e duhur. Nëse shkruani një artikull, fokusoni titullin tuaj dhe kopjoni atë që është e vërtetë, në vend që të thoni kryesisht atë që është e rreme. Studimet kanë treguar se përsëritja e gënjesh-trave mund t'i bëjë njerëzit të mbajnë (mend) informacionet e pasakta.

Roli juaj është të minimizoni sa më shumë që të jetë e mundur përsëritjen e të pavërtetave dhe t'i drejtoni njerëzit drejt informacionit të saktë.

Identifikimi i fjalëve kyçe dhe lokacioneve

Derisa ngjarja shpaloset, krijoni një listë vendndodhjesh (lokacionesh) dhe fjalëve kyçe relevante.

Për vendndodhjen, merrni parasysh qytetin, shtetin dhe vendin, si dhe çdo term përkatës lokal, si nofka për një qytet ose lagje të prekur. Gjatë zgjedhjeve, duhet po ashtu të përdorni edhe emrin e qarkut ose të zonës zgjedhore përkatëse. Ky informacion përdoret për të monitoruar postimet e gjeoetiketuara (geotagged) dhe për të kërkuar përmendjet e vendndodhjes. Gjithashtu, sigurohuni që të identifikoni dhe të filloni monitorimin e llogarive sociale të çdo autoriteti vendor relevant, siç janë policia dhe departamentet e zjarrfikësve, politikanët dhe mediat lokale të lajmeve.

Më pas, identifikoni termat kyç. Këta mund të përfshijnë fjalët si viktimë, i dyshuar, gjuajtës, të shtëna, përmbytje, zjarr, emrat e konfirmuar të kujtdo që është përfshirë dhe formulime më të përgjithshme si "kërkoj" - mendoni për gjuhën që do të përdornin njerëzit në situatë, përveç termave kyç. Nëse gjeni një llogari të besueshme që poston nga qendra e ngjarjes që po monitoroni, shënoni emrin e përdoruesit në tërësi feed-in e tyre. Shikimi i listës së miqve ose ndjekësve të tyre është gjithashtu një mënyrë e dobishme për të gjetur njerëz të tjerë në këtë zonë që mund të jenë prekur.

Vini re se gjatë situatave stresuese, njerëzit mund të shkruajnë gabimisht lokacionet ose emrat. Për shembull, gjatë zjarrit Kincade (Kinkejd) të vitit 2019 në Kaliforni, disa postuan në Twitter #kinkaidfire për shkak të korrigjimit automatik. Përfshini gabimet e zakonshme drejtshkrimore në kërkimet tuaja dhe përpiquni të identifikoni gabimet e mundshme të korrigjimit automatik duke shtypur fjalët kyçe në pajisjen tuaj duke parë se cilat sugjerime shfaqen.

Kjo është gjithashtu një kohë e mirë për të kontaktuar me çdo burim që njihni në vendndodhjen relevante ose që janë pjesë e komuniteteve që mund të jenë në shënjestër të ngacmimeve ose dezinformatave, dhe të pyesni se çfarë kanë parë onlajn. Mund t'i tregoni audiencës tuaj se jeni në kërkim të dezinformatave dhe përmbajtjeve tjera problematike që lidhen me ngjarjen. Koordinohuni me ekipin e mediave sociale të redaksisë suaj për të ndihmuar në përhapjen lajmit në lidhje me monitorimin tuaj dhe për të parë nëse ata kanë parë ndonjë gjë të rëndësishme.

Mjetet kyçe për imazhe

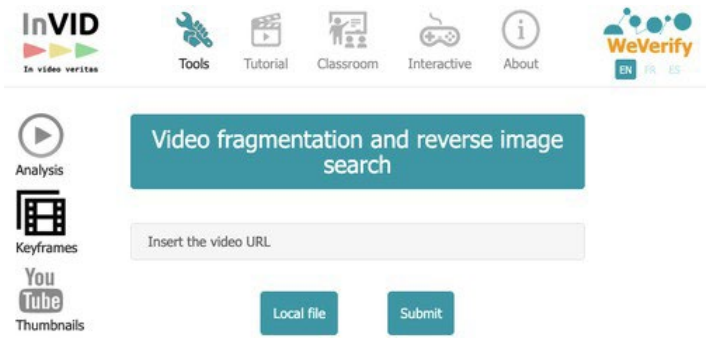
1. Kërkimi i imazheve

Kërkimi i kundërt i imazhit është një mjet i domosdoshëm. Është e lehtë të kërkosh një imazh në Google duke klikuar me të djathtën mbi imazhin dhe duke zgjedhur "Kërko Google për Imazh" ("Search Google for Image") në shfletuesin e internetit Chrome. Por është gjithmonë një ide e mirë të kërkoni një imazh duke përdorur mjete të ndryshme. Nëse instaloni ekstensionin e shfletuesit InVID, mund të klikoni me të djathtën mbi një imazh dhe ta kërkoni atë nëpër mjete të ndryshme. Ky grafik krahasimi i kërkimit të imazhit të kundërt i krijuar nga Domain Tools tregon përparësitë dhe dobësitë relevante të produkteve të ndryshme për kërkim të kundërt të imazhit:

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

InVID

InVID është shtesë falas e shfletuesve dhe platforma më e mirë për t'ju ndihmuar të analizoni dhe verifikoni videot. Ai u lejon përdoruesve të vendosin (paste) një URL në motorin e tij, i cili më pas do të ekstraktojë thumbnails-at nga videoja. Mund të kryeni kërkime të kundërta të imazheve në këto thumbnails-a për të parë se ku tjetër është shfaqur kjo video në ueb.



2. Kërkimi në TweetDeck

Mënyra më e mirë për ta kërkuar Twitterin është duke përdorur TweetDeck, i cili ju lejon të krijoni kolona unike për kërkime dhe lista.

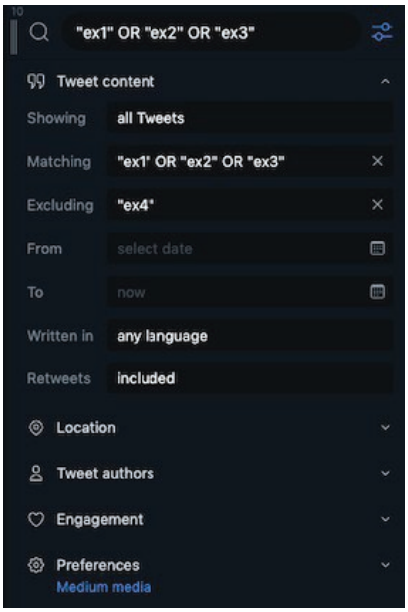
Gjetja dhe dyfishimi i listave relevante është kyçe për të qëndruar në kontroll të një situate. Mund të përdorni Google për të kërkuar listat në Twitter duke përdorur një formulë të thjeshtë. Shkruani "site:twitter.com/*/lists" në motorin e kërkimit dhe më pas shtoni një fjalë kyçe në thonjëza, për shembull "Alabama reporters" (Reporterët e Alabamës). Pra, stringu (zinxhiri) përfundimtar i kërkimit është:

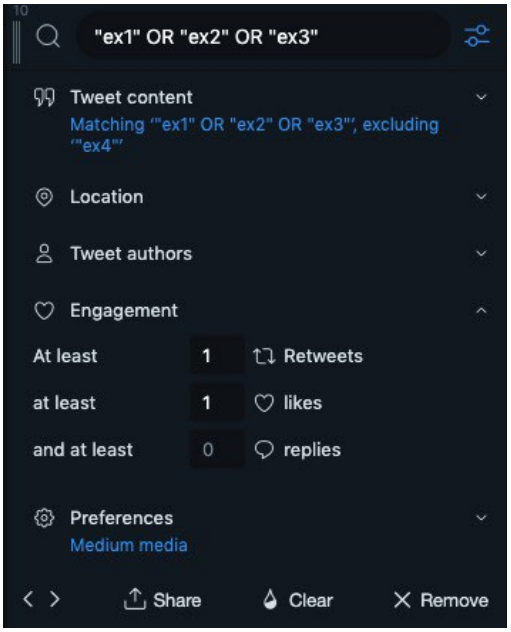
site:twitter.com/*/lists "Alabama reporters"

Kjo do të nxjerrë çdo listë që kanë e krijuar përdoruesit e tjerë të Twitterit, e cila në titull përfshin frazën "reporterët e Alabamës".

Pasi të keni gjetur një listë që është relevante për nevojat tuaja, duhet ta dyfishoni atë në mënyrë që të mund ta shtoni në TweetDeck. Përdoreni këtë aplikacion: http://projects.noahliebman.net/listcopy/connect.php për të dyfishuar aq sa dëshironi. Është ideale të dyfishoni një listë në vend që ta ndiqni, sepse mund të shtoni ose hiqni përdorues sipas dëshirës tuaj.

Së bashku me gjetjen dhe shtimin e listave në kolonat e TweetDeck-ut, dëshironi të krijoni kolona me filtra specifikë kërkimi që ju mundësojnë të monitoroni shpejt fjalët kyçe, si dhe imazhet dhe videot. Për të kërkuar më shumë fjalë kyçe, i vendosni ato në thonjëza dhe vendosni "OR" midis tyre, si "Kincade" OR "Kinkade". Ju gjithashtu mund çkyçni disa fjalë nëse ato japin rezultate të parëndësishme. Shumica e njerëzve nuk i etiketojnë më tuitet e tyre sipas lokacionit, kështu që ju mund ta lini atë fushë bosh për të hedhur një rrjet më të gjerë.





Nëse doni të ngushtoni rezultatet tuaja, vendosni fushën "From"(Nga) në një ose dy ditë përpara se të ketë ndodhur ngjarja, pasi kjo do të sigurojë që të mos humbisni tuitet për shkak të problemeve të mundshme me zonën kohore. Nëse ende merrni shumë rezultate, provoni t'i filtroni ato sipas angazhimit për të shfaqur vetëm postimet që të tjerët kanë pëlqyer ose rituituar. Mund të provoni gjithashtu t'i ndani termet kyçe në kolona të veçanta. Për shembull, vendosni lokacionet në një kolonë dhe fjalë kyçe të tjera në një kolonë tjetër. Unë zakonisht ndaj një kolonë të tretë për emrat e mundshëm të të dyshuarve ose viktimave dhe gabimet e tyre drejtshkrimore.

Së fundi, nëse po shihni një numër shumë të lartë tuitesh, është mirë të krijoni një kolonë të re me fjalët kyçe më të mira dhe të vendosni opsionin "Showing" (Të shfaqura) nën filtrin "Tweet content" (Përmbajtja e tuitit) për të shfaqur vetëm foto dhe video. Kjo do t'ju japë një feed që mund t'ju ndihmojë të vëreni pamjet virale ose të reja.

3. CrowdTangle

CrowdTangle është aplikacion uebi si dhe ekstension (shtesë) i kërkuesve që mund të përdoret nga redaksitë pa pagesë. (Kontaktojeni kompaninë nëse redaksia juaj nuk është regjistruar për të pasur qasje.)

Është një mjet i fuqishëm që ju lejon të krijoni panele (dashboards) që të monitoroni në Facebook, Instagram, dhe Reddit. Po ashtu, mund të kërkoni me fjalë kyçe dhe përcaktoni më shumë filterë, duke e përfshirë datën e postimit, gjuhën, dhe angazhimin (engagement). CrowdTangle është veçanërisht i dobishëm për monitorim të Facebookut dhe kontrollimit nëse një URL është publikuar në media sociale.

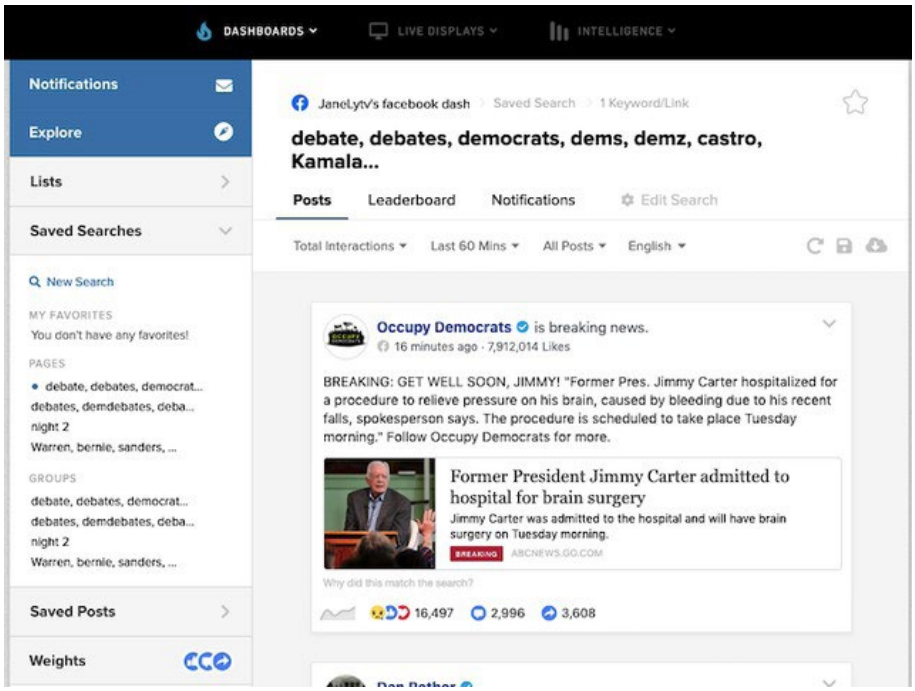
Menjëherë pasi të keni qasje, shkoni në app.crowdtangle.com që të filloni, e pastaj klikoni në "Create New Dashboard" (Krijoni panele të ri). Edhe nëse nuk keni qasje, ekstensioni i kërkuesit është pa pagesë për çdokënd që dëshiron ta përdorë.

CrowdTangle: Kërkimi i postimeve në Facebook

Klikoni në “Saved Searches” (kërkime të ruajtura) në shiritin anësor të majtë dhe pastaj në “New Search” (kërkim i ri). Keni dy opsione për Facebookun: search pages (kërkoni faqet) dhe search groups (kërkoni grupet). Do t’i rekomandoja të dyja. Futni sado fjalë kyçe që dëshironi duke i ndarë me presje. Pastaj mund ta përcaktoni se si t’i shikoni postimet, për shembull më të fundit (most recent), më të popullarizuarat (most popular) dhe ato me performanca më të larta (over-performing), që është njësi matëse e postimeve që marrin më shumë angazhim sesa që është normale për faqen e dhënë. Unë i kontrolloj të trija varësisht nga situata, që të sigurohem se i shoh përmbajtjet virale dhe ato të reja.

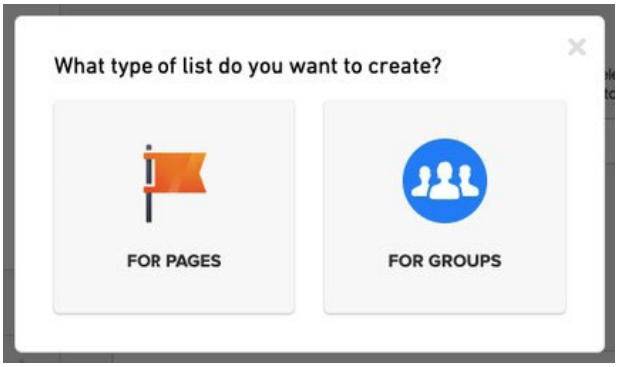
Gjithashtu mundeni t’i renditni postimet sipas një kornize kohore dhe lloji specifik. CrowdTangle së fundmi ka shtuar mundësinë për të kërkuar postime sipas lokacionit të faqes prej nga janë postuar. Pasi të klikoni në “English” (Anglisht), e pastaj ta zgjidhni “Country” (Vendi), mund të përzgjidhni vetëm postime që vijnë nga faqet që e kanë deklaruar lokacionin e tyre brenda ShBA-ve, për shembull. Po ashtu, mund ta bëni të kundërtën dhe të kërkoni postime që vijnë nga faqe të bazuara në Iran, Rusi, Arabi Saudite, Filipine ose Indi, për shembull. Mbani fokus veçanërisht në postimet e bazuara në imazhe dhe video, që kanë tendencë të shpërndahen më tej dhe të jenë më angazhuese.

Pasi ta keni caktuar kërkimin me rezultate relevante, sigurohuni ta ruani që të mund t’i riktheheni.



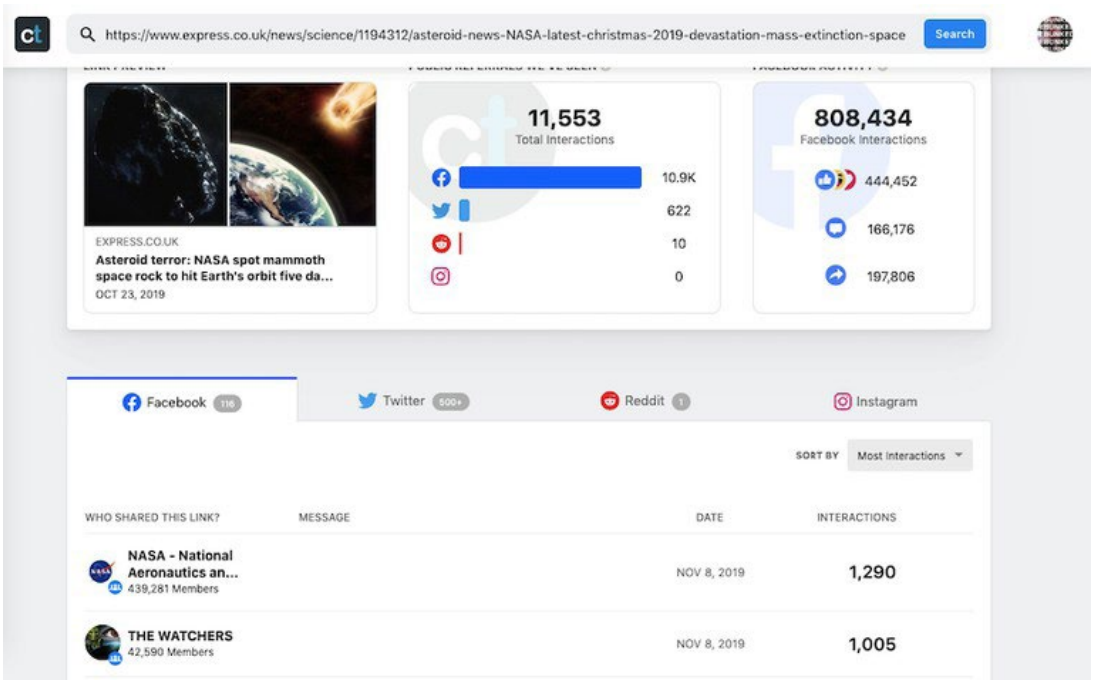
CrowdTangle: Listat

Sikur TweetDeck, CrowdTangle ju lejon të ndërtoni lista të faqeve dhe grupe publike sipas interesit. Duke klikuar në "Lists" në shiritin anësor të majtë dhe pastaj "Create list" (krijo listën), mund t'i monitoroni faqet ose grupet që përshtaten me fjalët kyçe që i keni zgjedhur ose me faqet të cilave ua keni URL-në. CrowTangle ka po ashtu një numër të madh të listave të ndërtuara paraprakisht që mund t'i shikoni duke klikuar në skedën (tabin) "Explore" (eksploro). Njësoj si me Twitterin, të ndërtuarit e listave të faqeve dhe grupeve që flasin për ngjarjen që jeni duke e mbuluar është mënyrë e mirë ta monitoroni ambientin e informacionit.\



CrowdTangle: Kërkimi i linqeve

Një veçori tjetër relevante e CrowdTangle është kërkimi i linkut.
Shkoni në https://apps.crowdtangle.com/search/ dhe kopjoni (paste) brenda URL-në ose në fjalët kyçe të përmbajtjeve që ju interesojnë. CrowdTangle do t'ju shfaqë shpërndarësit më të popullarizuar publik (top public sharers) të linkut në Facebook, Instagram, Reddit dhe Twitter (vini re se rezultatet e Twitterit janë të kufizuara në shtatë ditët e kaluara). Kjo do t'ju ndihmojë të kuptoni se si është duke u shpërndarë përmbajtja, nëse ka grupe apo individë që duhet t'i hulumtoni më tej, dhe në qoftë se përmbajtja është shpërndarë mjaftueshëm sa që kërkon një përgënjeshtrim. Nuk ka rregulla të thjeshta se kur duhet ta përgënjeshtrojmë një të pavërtetë, por disa pyetje të mira për këtë janë: A është shpërndarë jashtë rrjetit fillestar të shpërndarësve? A është shpërndarë nga figura me autoritet? A ka gjeneruar angazhim të rëndësishëm? (Shtesa pa pagesë e kërkuesit i jep të dhënat e njëjta sikurse mjeti i kërkuesit të linkut, dhe të dyja janë pa pagesë për t'u përdorur nga çdokush pa pasur llogari të plotë në CrowdTangle).

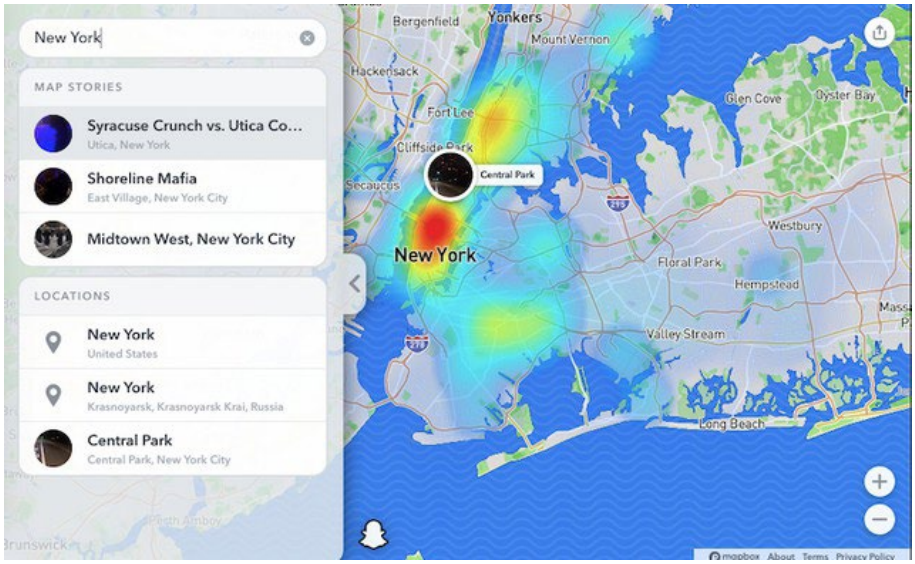


4. Instagram.com

Instagrami është vend i dobishëm për të monitoruar hashtagjet dhe postimet e gjeoetiketuara. Shikoni lokacionet relevante ku përdoruesit mund të kenë etiketuar fotografi, dhe mbani mend që etiketimet e lokacionit mund të përfshijnë gjithashtu fqinjët dhe pikat e referimit (landmarks). Pasi ta keni gjetur dikë që duket se ka qenë i përfshirë në një ngjarje lajmi, klikoni në llogarinë e tyre dhe sigurohuni që t'i përcillni storiet (story) e tyre – ato janë shumë më të popullarizuara sesa postimet e zakonshme të Instagramit. Gjithashtu shikoni edhe në komentet për dëshmitarë tjerë potencial, dhe vëreni çdo hashtag që mund të jetë përdorur përgjatë postimeve të tyre. Nëse dëshironi të arkivoni story-n e Instagramit të dikujt për dosjet tuaja, mund të përdorni uebfaqe si storysaver.net për ta zbritur atë.

5. SnapMap

Dezinformatat në Snapchat janë të pazakonshme, por mjeti i hartës publike (public map) i këtij rrjeti është i dobishëm për të ndihmuar në verifikimin apo zbulimin e mashtrimeve. Për të filluar, shkoni në map.snapchat.com futni lokacionin që ju intereson. Kjo do t'ju tregojë një hartë "të nxehtësisë" (heat map) se ku janë duke u publikuar përmbajtjet – sa më i ndritshëm është lokacioni, aq më shumë Snap-a vijnë nga atje. Për të ruajtur një Snap të dobishëm, klikoni në tre pikat lartë në të djathtë dhe përzgjedhni "Share" (Shpërndaj). Do të keni mundësi ta kopjoni URL-në e Snap-it për ta shikuar më vonë. (Sigurohuni që po ashtu të bëni edhe një skrinshot).



Kur përmblidhen të gjitha bashkë

Është thelbësore ushtrohet përdorimi i çdo mjeti para se të dalë lajmi i fundit, për të shmangur ngatërrimet në moment. Dezinformatat kanë për qëllim bëjnë lojë me emocionet dhe të kapitalizojnë mbi zbrazëtirat e mbulimit të lajmeve. Mbani mend këtë derisa kërkoni në ueb. Po ashtu, do të hasni shpesh edhe informacione të sakta që mund t'u ndihmoj; kolegëve tuaj. Shkruani çdo gjë që dini se është e vërtetë që të mund t'i vëreni më shpejtë të pavërtetat, dhe mos hezitoni të kërkoni ndihmë prej ndonjë reporteri të medias suaj që është në terren.

Pasi që të "bjerë pluhuri" (të qartësohet ose të përfundojë situata), është e nevojshme të shikoni prapa në imazhet the postimet që i keni ruajtur. Përderisa në moment dëshironi t'i vini në dukje të pavërtetat individuale sipas parimeve të gazetarisë së shërbimit publik, pas kësaj duhet të bëni një bilanc të çdo teme ose paterni (modeli) që mund të shihet. A janë targetuar njerëzit sipas racës apo gjinisë? A janë bërë mejnstrim mashtrimet që buruan nga llogari të vogla anonime? A kanë vepruar kompanitë e mediave sociale veçanërisht mirë apo veçanërisht dobët? Një storie përmbledhëse mund t'u ndihmojë lexuesve tuaj për ta kuptuar në tërësi qëllimin dhe metodat e shpërndarjes së dezinformatës. Po ashtu, do të shërbejë edhe si mjet hulumtimi për ju dhe redaksinë tuaj, duke ju treguar se çfarë mund të jetë e dobishme që të fokusoheni herën e ardhshme kur të dalë ndonjë lajm i fundit.

5. Verifikimi dhe hetimi i imazheve

Shkruajnë: Hana Gaj, Farida Vis , Simon Fokner

Farida Vis *(Farida Vis) është drejtoreshë e Visual Social Media Lab dhe profesoreshë e mediave digjitale në Universitetin Metropolitan të Mançesterit. Puna e saj akademike dhe në gazetarinë e të dhënave fokusohet në përhapjen e dezinformatave onlajn. Ajo ka shërbyer në Këshillin e Agjendës Globale për Mediat Sociale të Forumit Ekonomik Botëror (2013-2016) dhe në Këshillin Global të Ardhmërisë për Informacion dhe Argëtim (2016-2019), dhe është drejtoreshë në Open Data Manchester.*

Simon Fokner *(Simon Faulkner) është ligjërues i historisë së artit dhe kulturës pamore në Universitetin Metropolitan të Mançesterit. Hulumtimi i tij ka të bëjë me përdorimet politike dhe kuptimet e imazheve, me një fokus të veçantë në aktivizmin dhe lëvizjet protestuese. Ai është gjithashtu ko-drejtor i Visual Social Media Lab (Laboratori Vizual i Mediave Sociale) dhe ka një interes të fuqishëm mbi zhvillimin e metodave relevante për analizën e imazheve të qarkulluara në mediat sociale.*

Hana Gaj *(Hannah Guy) është doktorante në Universitetin Metropolitan të Mançesterit, ku ekzaminon rolin e imazheve në përhapjen e dezinformatave në mediat sociale. Ajo është anëtare e Visual Social Media Lab, ku projektet e saj aktuale eksplorojnë imazhe të shpërndara në Twitter gjatë shfaqjes së lëvizjes Black Lives Matter, dhe Edukimin Mediatik Vizual (Visual Media Literacy) për të luftuar keqinformimin në kontekstin e shkollave kanadeze.*

Komunikimi në mediat sociale tani është në masë të madhe vizual. Fotografitë dhe videot janë bindëse, tërheqëse dhe më të lehta për t'u krijuar se kurrë, dhe mund të nxisin reagime të fuqishme emocionale. Si rezultat, ato janë kthyer në mjete të fuqishme të keqinformimit dhe dezinformimit.

Deri më sot, diskutimi mbi imazhet brenda kontekstit të keqinformimit dhe dezinformimit është përqendruar ose në teknikat e verifikimit ose, së fundmi, është fokusuar në mënyrë disproporcionale në deep-fake videot (video mashtruese të krijuara me ndihmën e programeve kompjuterike). Përpara se të shqyrtojmë deepfake-t, siç bëjmë në kapitullin e radhës, është thelbësore të kuptojmë përdorimin më të zakonshëm të teknologjisë së ulët për prodhim të fotografive dhe videove mashtruese, veçanërisht atyre që janë të nxjerra jashtë kontekstit.

Duke pasur parasysh përdorimin e gjerë të pamjeve në tentimet për të ndikuar dhe manipuluar diskursin publik, gazetarët duhet të pajisen me njohuri themelore të verifikimit të imazhit dhe me aftësinë për të vënë në pyetje dhe për të vlerësuar në mënyrë kritike imazhet që të kuptojnë se si dhe pse ato përdoren. Ky kapitull përqendrohet në zhvillimin e këtij grupi të dytë të aftësive dhe përdor një kornizë veprimi që e kemi zhvilluar në Visual Social Media Lab.

Ndërtimi në bazë të verifikimit

Në Visual Social Media Lab, fokusohemi në të kuptuarit e roleve që luajnë onlajn imazhet brenda shoqërisë. Ndërsa fokusohemi kryesisht në imazhe statike, kjo përfshin gjithashtu një sërë llojesh të ndryshme imazhesh: fotografi, imazhe të përbëra, meme, imazhe grafike dhe skrinshote, për të përmendur disa. Trajtimi i informatave të gabuara (misinformatave) dhe dez-informatave vizuale kërkon një grup të veçantë të strategjive. Deri më sot, verifikimi i imazheve nga gazetarët është fokusuar në përcaktimin nëse imazhi është ai që ata mendojnë se është. Në "Doracakun e Verifikimit" origjinal, Trushar Barot përshkroi katër parime bazë thelbësore për verifikimin e imazhit, të cilat mbeten tejet të çmueshme. Drafti i parë i Udhëzuesit të verifikimit vizual (First Draft Visual Verification Guide) është një burim tjetër i dobishëm që përdor këto parime duke u fokusuar në pesë pyetje për fotot dhe videot:

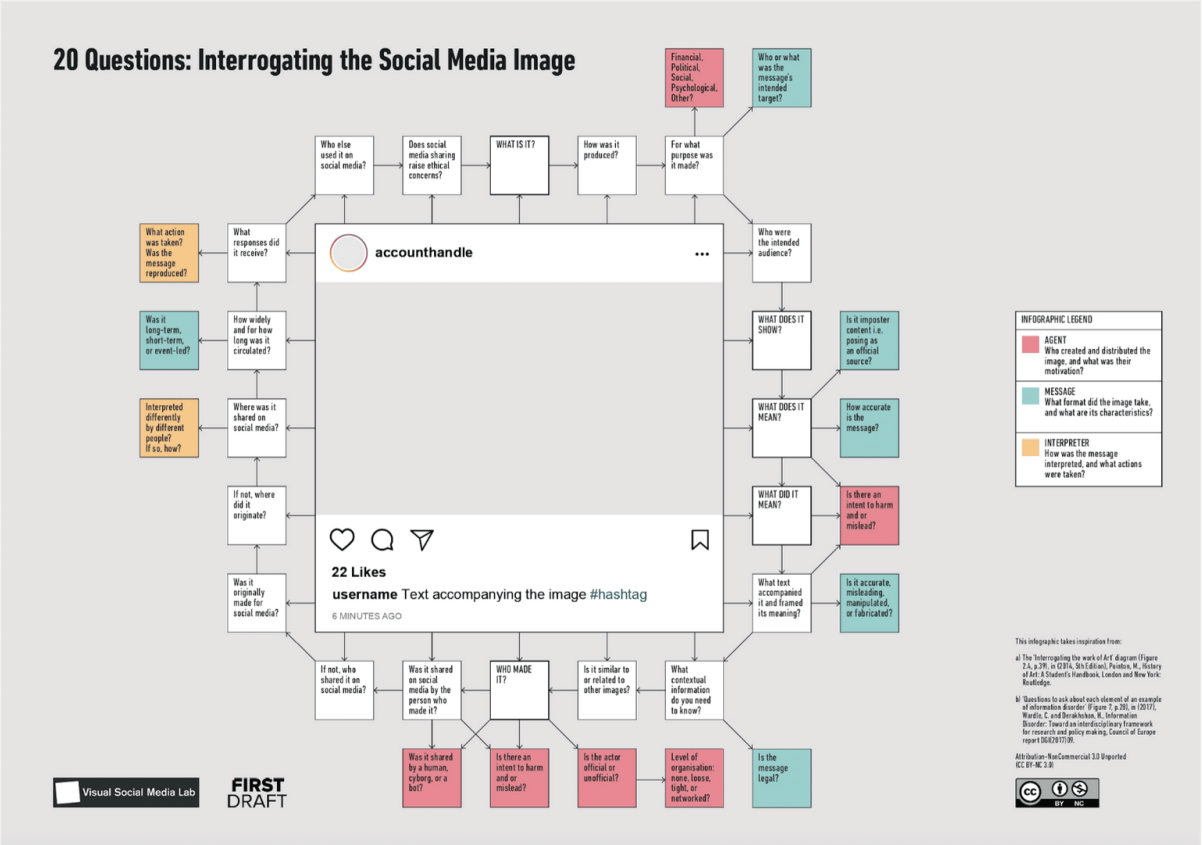
1. A po e shikoni versionin origjinal?
2. A e dini se kush e ka bërë foton?
3. A e dini se ku është shkrepur fotografia?
4. A e dini se kur është shkrepur fotografia?
5. A e dini pse është bërë fotografia?

Mjetet standarde që mund të ndihmojnë me hetimin e fotove dhe videove përfshijnë InVID, Yandex Image Search, TinEye, Google Image Search dhe Forensically. Këto metoda verifikimi fokusohen në origjinën e imazhit.

Ndërsa kjo metodë mbetet thelbësore, strategjitë dhe teknikat e përdorura shpesh në keqin-formim dhe dezinformim, si dhe në një sërë formash të manipulimit të medias, nënkuptojnë gjithashtu se është e rëndësishme të merret parasysh se si përdoren dhe shpërndahen imazhet dhe nga kush, dhe gjithashtu çfarë roli luajnë gazetarët në amplifikimin potencial të mëtejshëm të imazheve problematike.

Për të shkuar përtej formave standarde të verifikimit të imazhit, kemi kombinuar metoda nga historia e artit me pyetje të krijuara posaçërisht për përmbajtje keqinformuese (misinformuese) dhe dezinformuese. Korniza jonë, "20 pyetje për hetimin e imazheve të mediave sociale", e krijuar në bashkëpunim me First Draft dhe me gazetarë, është një mjet shtesë që mund ta për-dorin gazetarët kur hetojnë imazhet.

Hetimi i imazheve të mediave sociale



Siç sugjeron titulli, korniza përbëhet nga 20 pyetje që mund të bëhen për çdo imazh të mediave sociale (imazhe të palëvizshme, video, gif, etj.), me 14 pyetje shtesë që synojnë të gërmojnë më thellë në aspekte të ndryshme të misinformatave dhe dezinformatave. Pyetjet nuk shfaqen në një rend të caktuar, por këto pesë pyetje janë të dobishme për t'u adresuar fillimisht:

1. Çfarë është kjo?
2. Çfarë tregon?
3. Kush e ka bërë?
4. Çfarë do të thoshte më parë?
5. Çfarë do të thotë tani?

Pyetjet 1 deri në 3 janë të ngjashme me qasjet e etabluara për verifikim dhe kanë të bëjnë me përcaktimin se për çfarë lloji të imazhit flitet (një fotografi, video, etj.), çfarë ai përshkruan dhe kush e ka bërë atë. Megjithatë, pyetjet 4 dhe 5 na çojnë diku tjetër. Ato prezantojnë konsiderata të kuptimit që përfshijnë atë që tregon imazhi, por gjithashtu mbulojnë çdo kuptim të prodhuar nga përdorimi i imazhit, duke përfshirë edhe ato që bëhen nga identifikimi i tij të gabuar. Kur mendohet për të gjitha së bashku, pyetjet 4 dhe 5 na lejojnë gjithashtu të përqendrohemi në ndryshimin e natyrës së kuptimit të imazheve dhe në mënyrat se si kuptimet që u atribuohen imazheve, nëpërmjet ripërdorimit, mund të bëhen të rëndësishme në vetvete. Kjo nuk ka të bëjë thjesht me atë se çfarë kuptimi është dashur të kenë imazhet në një kontekst të ri dhe se si kjo e keqidentifikon atë që ato tregojnë, por edhe me atë se cilat janë efektet e keqidentifikimeve të tilla. Kjo qasje nuk ka të bëjë më me verifikimin, por më shumë me analizën e kuptimeve të imazheve të kryera në disiplina si historia e artit dhe teoria e fotografive.

Në zhvillimin dhe përdorjen e hershme të kësaj kornize me gazetarët, dëgjuam shpesh se ata kurrë nuk kishin menduar për imazhet me kaq shumë detaje. Shumë prej tyre thanë se korniza u ka ndihmuar të kuptonin se imazhet janë forma komplekse komunikimi dhe se kërkohet një metodë e qartë për t'i vënë në pyetje ato dhe kuptimin e tyre.

Në shumicën e rasteve, nuk do t'ju duhet t'u përgjigjeni të gjitha 20 pyetjeve në kornizën punuese për të marrë një kuptim gjithëpërfshirës të asaj që po ndodh me një imazh. Pyetjet janë aty për t'ju kthyer përsëri. Në punën tonë, kemi gjetur se ato janë veçanërisht të dobishme kur kemi të bëjmë me imazhe dhe video komplekse të profilit të lartë të lajmeve që kanë marrë vëmendje dhe shqyrtim të konsiderueshëm të medias. Për të treguar se si duket kjo në praktikë, këtu janë tre studime rasti me shembuj të profilit të lartë nga Mbretëria e Bashkuar dhe SHBA.

Rast Studimi 1: *Breaking Point (Pika kthyese), Qershor 2016*

Çfarë është kjo?

Imazhi "Breaking Point" ishte një poster i përdorur nga Partia e Pavarësisë së Mbretërisë së Bashkuar (UKIP) si pjesë e fushatës së saj gjatë referendumit të BE-së të vitit 2016. Ai përdorte një fotografi të bërë nga fotoreporteri Jeff Mitchell në tetor 2015, që fokusohej në krizën e refugjatëve.

Çfarë tregon?

Një radhë e madhe refugjatësh sirianë dhe afganë janë të shoqëruar nga policia sllovene nga kufiri midis Kroacisë dhe Sllovenisë deri në kampin e refugjatëve në Brezice. Posteri përdorte një version të prerë (të kropuar) dhe kishte të shtuar tekstin "PIKË KTHYESE: BE-ja na ka zhgënjyer (dështuar) të gjithëve" dhe "Duhet të çlirohemi nga BE dhe të marrim prapa kontrollin e kufijve tanë". Për shkak se refugjatët duket se lëvizin masivisht drejt shikuesit, kjo ka një ndikim të fortë vizual.

Kush e ka bërë?

Firma reklamuese me qendër në Edinburg, Family Advertising Ltd., e cila u angazhua nga UKIP për fushatën e saj të Brexit-it.

Çfarë do të thoshte më parë?

UKIP nuk u përpoq të keqinterpretonte përmbajtjen, por shtresoi kuptim të mëtejshëm duke shtuar slogane. Duke shfrytëzuar sentimentet ekzistuese anti-imigrante dhe raciste, ky manipulim u përqendrua në gjenerimin e frikës së mëtejshme nga imigrimi dhe refugjatët, mbi bazën e pretendimeve dhe insinuatave të pabaza në lidhje me politikën kufitare të BE-së.

Çfarë do të thotë tani?

Në nëntor të vitit 2019, në prag të zgjedhjeve të përgjithshme në Mbretërinë e Bashkuar, organizata e fushatës Leave.EU përdori gjithashtu një version të kropuar ngushtë të fotografisë në një imazh kundër imigracionit të ngarkuar në Twitter, duke bërë një referencë të qartë në posterin e UKIP-it të vitit 2016.

Cilat pyetje të tjera janë të dobishme për të bërë?

A është aktori zyrtar apo jozyrtar? Aktori kyç në krijimin dhe shpërndarjen e imazhit, UKIP, është një parti politike zyrtare, e jo një lloj aktori që zakonisht shoqërohet me misinformata dhe dezinformata.

A është e ngjashme ose në relacion me imazhe të tjera? Disa e krahasuan posterin me propagandën naziste; ai rezonon si me imazhet e mëparshme anti-migrante ashtu edhe me një histori më të gjatë të posterëve politikë në Mbretërinë e Bashkuar që përfshinin radhë të njerëzve, duke përfshirë atë të përdorur nga UKIP në maj 2016, i fokusuar në imigracionin nga BE.

3 përfundime kyçe:

- Partitë politike zyrtare dhe politikanët zyrtarë mund të jenë aktorë në përhapjen e informatave të gabuara (misinformatave).
- Misinformimi (informimi i gabuar, keqinformimi) nuk përfshin domosdoshmërisht imazhe të rreme apo edhe keqidentifikim të asaj që ato tregojnë. Ndonjëherë imazhet mund të përdoren për të mbështetur një mesazh që keqinterpreton një situatë më të gjerë.
- Disa misinformata kërkojnë më shumë se verifikim. Ekziston nevoja për të shqyrtuar në mënyrë kritike se si imazhet reale përdoren për të manipuluar, dhe çfarë bëjnë dhe çfarë kuptimi kanë imazhet e tilla.

Shembuj të mbulimit mediatik të këtij rasti:

Posteri anti-migrant i Nigel Forage u raportua në polici
(Nigel Forage's anti-migrant poster reported to police — The Guardian)

Brexit: Posteri 'joetik' kundër imigracionit i UKIP
(Brexit: UKIP's 'unethical' anti-immigration poster —Al-Jazeera)

Nigel Farage akuzohet se ka përdorur propagandë të stilit nazist, teksa fushata për Mbetje e pengon shpalosjen e posterit me furgonët rivalë (Nigel Farage accused of deploying Nazi-style propaganda as Remain crash poster unveiling with rival vans — The Independent)

Rast studimi 2: *Fotografia e Urës së Uestminsterit, mars 2017*

Çfarë është kjo?

Një tuit nga një llogari në Twitter që duket se drejtohet nga një burrë i bardhë nga Teksasi, i cili mori vëmendje të konsiderueshme mediatike. Më vonë u zbulua se llogaria operohej nga Agjencia Ruse e Kërkimeve të Internetit, dhe u përdor për të përhapur misinformata dhe dez-informata. Tweet shpërndau një fotografi nga pasojat e sulmit terrorist të urës Uestminster (Westminster) në Londër (22 mars 2017).

Çfarë tregon?

Një grua myslimane duke kaluar pranë një grupi njerëzish dhe një personi të shtrirë në tokë, i cili është lënduar në sulmin terrorist. Teksti ka konotacione islamofobike, duke pretenduar se gruaja po injoron qëllimisht personin e lënduar, si dhe një hashtag haptazi anti-islamik.

Kush e ka bërë?

Punonjësi i Agjencisë së Kërkimeve të Internetit që drejtonte llogarinë @SouthLoneStar në Twitter, megjithëse nuk dihej se kjo ishte një llogari e IRA-s në kohën kur u bë postimi në Twit-ter. Vetë fotografia është bërë nga fotoreporteri Xhejmi Lorimen (Jamie Lorriman).

Çfarë do të thoshte më parë?

Në mars të vitit 2017, ky dukej të ishte një tuit nga një përdorues i Twitter-it i djathtist nga Tek-sasi, i cili e interpretoi fotografinë se ajo gjoja tregonte se gruaja myslimane nuk kujdesej për personin e lënduar. Postimi sugjeronte se ky shembull fliste për një të vërtetë më të madhe rreth myslimanëve.

Çfarë do të thotë tani?

Që sot, tuiti është dëshmi e përhapjes së qëllimshme të dezinformatave islamofobike nga Ag-jencia e Kërkimeve në Internet në kohën pas një sulmi terrorist.

Cilat pyetje të tjera janë të dobishme për t'u bërë?

Çfarë reagimesh mori? Ky postim në Twitter mori reagime të rëndësishme nga mediat me ndik-im. Dhjetëra gazeta në Mbretërinë e Bashkuar raportuan për të, në disa raste më shumë se një herë. Ndërsa shumica e këtyre artikujve dënuan @SouthLoneStar, kjo gjithashtu e zhvendosi

tuitin nga kufijtë e mediave sociale dhe e hapi atë për një mejnstrim audiencë. Pas përhapjes së imazhit, gruaja në foto foli publikisht për të thënë se ishte e shqetësuar për sulmet në atë kohë dhe se "jo vetëm që kam e tronditur duke parë pasojat e një sulmi terrorist tronditës dhe mpirës, por gjithashtu duhej të përballesha me tronditjen e gjetjes së fotografisë sime të suvatuar anembanë mediave sociale nga ata që nuk mund të shikonin përtej veshjes sime, të cilët nxjerrin përfundime të bazuara në urrejtje dhe ksenofobin."

A është e ngjashme ose në relacion me imazhe të tjera? Imazhi që qarkullonte në të shumtën e rasteve ishte një nga shtatë imazhet të bëra të gruas. Imazhet tjera tregonin qartë se ajo ishte e shqetësuar, diçka që u kap prej pak publikimeve.

Sa gjerësisht dhe për sa kohë ka qarkulluar? Vëmendja e shtuar e mediave me ndikim do të thotë që tuiti u përhap gjerësisht. Megjithatë, brenda pak ditësh, qarkullimi u ngadalësua ndjeshëm. Ai u riqarkullua në nëntor 2017, kur u zbulua se @SouthLoneStar operohej nga Agjencia e Kërkimeve në Internet. Ky qarkullim i mëvonshëm i nëntorit ishte dukshëm më i vogël në mediat me ndikim në krahasim me muajin mars.

3 përfundime kyçe:

- Dezinformatat vizuale nuk janë gjithmonë tërësisht të rremë dhe mund të përfshijnë elementë që bazohen në të vërtetën. Fotografia është reale, por konteksti i saj është manipuluar dhe falsifikuar, dhe mbështetet tek lexuesi/shikuesi që nuk e di se çfarë po mendonte në të vërtetë gruaja në atë moment.
- Gazetarët duhet të mendojnë me kujdes vallë do t'u sjellin vëmendje të mëtejshme dezinformatave të tilla të nxitura emocionalisht, të kontroverse dhe potencialisht të dëmshme duke raportuar mbi to, qoftë edhe me qëllime pozitive.
- Më shumë vëmendje mund t'i kushtohet korrigjimit të lajmeve të bazuara në dezinformata dhe sigurimit që pamja e vërtetë e ngjarjeve të jetë më e spikatur. Mbulimi i kufizuar në nëntor do të thotë se disa lexues mund të mos e kenë marrë vesh se tuiti ishte dezinformatë ruse.

Shembuj të mbulimit mediatik të këtij rasti:

Njerëzit po bëjnë supozime alarmante për këtë foto të 'gruas me shami duke ecur pranë një burri që po vdes' (People are making alarming assumptions about this photo of 'woman in headscarf walking by dying man' — Mirror)

"Kush është përbindëshi i vërtetë?" Interneti ballafaqohet me trollët që kritikuan një grua myslimane 'indiferente' që shihet duke kaluar nëpër sulme terroriste ('Who is the real monster?' Internet turns on trolls who criticised 'indifferent' Muslim woman seen walking through terror attack — Daily Mail)

Deputeti britanik i bën thirrje Twitter-it të publikojë tuitet e 'fabrikës së trollëve' rusë (British MP calls on Twitter to release Russian 'troll factory' tweets — The Guardian)

Rast studimi 3: *Konfrontimi te Memoriali i Linkolnit, janar 2019*

Çfarë është kjo?

Një video e një grupi nxënësish nga Shkolla e Mesme Katolike Covington që morën pjesë në Marshin për Jetën (pro-jetë e kundër abortit) dhe një indigjeni, Nejtën Filips (Nathan Phillips), i cili po shoqëronte amerikanët e tjerë indigjenë në Marshimin e Popujve Indigjenë.

Çfarë tregon?

Një përballje mes njërit prej nxënësve të Shkollës së Mesme Katolike Covington dhe Fillipsit. Dy demonstratat u mblodhën në Plaza (shesh), me një grup të madh nxënësve të Covington që mbanin kapela MAGA, për të cilët u supozua se u përballën me Fillipsin. Kjo përshkruan një pamje të një amerikani të vetmuar indigjen që përballet me një turmë të rinjsh bullizues të së djathtës radikale (alt-right).

Kush e ka bërë?

Videoja u ngarkua për herë të parë në Instagram nga një pjesëmarrës i Marshit të Popujve Indigjenë. Kjo mori rreth 200,000 shikime. Disa orë më vonë, videoja u ngarkua në Twitter, duke marrë 2.5 milionë shikime përpara se të fshihej nga llogaria origjinale. Videoja u ripostua më pas në faqe të ndryshme të mediave sociale, duke tërhequr më pas vëmendjen e mediave me ndikim. Brenda 24 orëve ishin publikuar disa artikuj për videon.

Çfarë do të thoshte më parë?

Narrativa fillestare që u përhap në internet e prezantoi videon si një përballje të drejtpërdrejtë midis Filipsit dhe nxënësve, në të cilën nxënësit shiheshin duke u tallur dhe duke u tubuar kërcënueshëm rreth Fillipsit.

Çfarë do të thotë tani?

Një video shumë më e gjatë e ballafaqimit, e cila u shfaq disa ditë pas videos së parë, pikturoi një pamje më komplekse. Memoriali u pushtua gjithashtu nga një grup izraelitësh të zinj hebrenj, të cilët po talleshin me kalimtarët, duke përfshirë nxënësit e Covington-it dhe pjesëmarrësit e Marshit të Popujve Indigjenë. Kjo çoi në një konfrontim të nxehtë midis të tre grupeve, përderisa Fillipsi supozohet se po përpiqej të qetësonte situatën. Këtu është momenti kur fillon videoja e parë.

Cilat pyetje të tjera janë të dobishme për t'u bërë?

Çfarë informacioni kontekstual duhet të dini?

Pa videon më të gjatë dhe pa dijeninë që izraelitët hebrenj të zinj ishin të pranishëm dhe që nxitën në mënyrë aktive konfliktin, i gjithë konteksti humbet. Përderisa nxënësit u regjistruan duke thënë gjëra raciste, ajo që çoi në këtë ishte më e ndërlikuar sesa thjesht adoleshentët e së djathtës radikale që grupoheshin kërcënueshëm kundër një burri të moshuar indigjen.

Ku u shpërnda në rrjetet sociale?

Ndërsa videoja fillimisht u shpërnda në Instagram nga dikush që mori pjesë në Marshimin e Popujve Indigjenë, kjo mori vëmendje të kufizuar. Më pas u ri-ngarkua në Twitter dhe YouTube nga përdorues të tjerë, gjë që amplifikoi ndjeshëm njohjen me rastin dhe siguroi vëmendjen e mediave me ndikim. Gjegjësisht, vëmendja erdhi nga këto ringarkime dhe jo nga videoja origjinale në Instagram.

3 përfundime kyçe:

- Kur pamje të tilla të ngarkuara me emocione përhapen kaq shpejt onlajn, është e lehtë të humbasësh kontekstin dhe të lejosh që tregimi sipërfaqësor dhe reaksionar në internet të marrë kontrollin.
- Në retrospektivë, disa gazetarë argumentuan se artikujt fillestarë shërbyen për të nxitur kontroversitetin dhe për të shtyrë më tej narrativën e pasaktë. Kjo sugjeron se pa hetimin e duhur, mediat me ndikim mund të vazhdojnë pa dashje përhapjen e misinformatave (informatave të gabuara).
- Shpejtësia me të cilën u përhap videoja onlajn nënkuptoi që shumë media me ndikim "ranë pre" e narrativës që shtyhej në mediat sociale dhe nuk hetuan më tej. Shumë faqe lajmesh u detyruan të tërhiqnin ose të korrigjonin artikujt e tyre pasi dolën të vërtetat për ngjarjen, dhe disa prej tyre u paditën.

Shembuj të mbulimit mediatik të këtij rasti:

Veterani indigjen amerikan i Vietnamit, i tallur dhe i rrethuar nga adoleshentë me kapele MAGA (Native American Vietnam Vet Mocked And Surrounded By MAGA Hat-Wearing Teens — UNILAD)

Revoltë pasi studentët me kapela Maga tallen me veteranin indigjen amerikan (Outcry after Kentucky students in Maga hats mock Native American veteran — The Guardian)

Videoja më e plotë hedh dritë të re mbi ballafaqimin e studentëve katolikë të Covington me të moshuarin vendas amerikan (Fuller video casts new light on Covington Catholic students' encounter with Native American elder — USA Today)

Përfundim

Shumë nga gjërat që shpërndahen në mediat sociale janë vizuale. Gazetarët duhet të pajisen me aftësinë për të vënë në pyetje dhe për të vlerësuar në mënyrë kritike imazhet, për të zbuluar përmbajtje dhe synime të rëndësishme. Shpejtësia me të cilën mund të përhapet misinformata vizuale thekson më tej nevojën që gazetarët të vazhdojnë punën me kujdes dhe të sigurohen që të hetojnë plotësisht storiet e lidhura me imazhe përpara se të publikohen. "20 Pyetjet për hetimin e imazheve të mediave sociale" është një mjet shtesë që gazetarët mund ta përdorin kur hulumtojnë imazhe, veçanërisht kur një storie përqendrohet kryesisht në diçka vizuale. Jo çdo pyetje nga korniza është e rëndësishme për çdo imazh, por pesë pyetjet bazë janë një pikënisje e fortë dhe bazohen në aftësitë themelore të verifikimit, me synim për të zhvilluar raportim më të saktë dhe më të thelluar.

SHTOJCË

Më poshtë është lista e plotë e pyetjeve nga Korniza e 20 Pyetjeve, duke përfshirë 14 pyetje të shkurta të menjëhershme që fokusohen në mënyrë specifike në misinformata dhe dezinformata. Siç kemi vërejtur në kapitull, janë pesë pyetje që janë të dobishme për t'u trajtuar së pari (me shkronja të trasha/bolduara). Pyetjet e menjëhershme lidhen ose me agjentin, ose me mesazhin, ose me interpretuesin e informatës së gabuar (misinformatës) dhe dezinformatës:

- AGJENTI (A) - Kush e krijoi dhe e shpërndau imazhin dhe cili ishte motivimi i tyre?
- MESAZHI (M) - Çfarë formati mori imazhi dhe cilat janë karakteristikat e tij?
- INTERPRETUESI (I) - Si u interpretua mesazhi dhe çfarë veprimesh u ndërmorën?

Çfarë është kjo?
Si është prodhuar?
Me çfarë qëllimi është bërë?
A - Financiar, Politik, Shoqëror, Psikologjik ose Tjetër?
M – Kush ose çka ka qenë caku i synuar i mesazhit?
Cili ka qenë publiku i synuar?
Çfarë tregon?
Çfarë do të thotë tani?
M – A është përmbajtje mashtruese, p.sh. duke aktruar burim zyrtar?
M – Sa i saktë është mesazhi?
Çfarë do të thoshte më parë?
a. A – A ka qëllim për të bërë dëm ose për të çorientuar?
Me çfarë teksti është shoqëruar dhe çfarë domethënie i është dhënë?
a. M – A është e saktë, çorientuese, e manipuluar ose e fabrikuar?
Çfarë informacioni kontekstual duhet të dini?
a. M – A është mesazhi legal?
A është i ngjashëm ose në lidhje me imazhe tjera?
Kush e ka bërë?
A – A është aktori zyrtar ose jozyrtar?
A – Niveli i organizimit: nuk ka, i dobët, i shtrënguar, ose i rrjetëzuar?
A është shpërndarë në media sociale nga personi që e ka bërë?
A – A është shpërndarë nga një njeri, një kiborg?
A – A ka qëllim për të bërë dëm ose për të çorientuar?
Nëse jo, kush e ka shpërndarë atë në media sociale?
A është bërë origjinalisht për media sociale?
Nëse jo, prej ku e ka origjinën?
Ku është shpërndarë në media sociale?
a. I – Interpretohet ndryshe nga njerëz të ndryshëm? Nëse po, si?
Sa gjerë deh për sa kohë ka qarkulluar?
a. M – A ka qenë afatgjatë, afatmesëm, apo i nxitur nga ndonjë ngjarje?
Çfarë reagimesh ka marrë?
a. I – Çfarë veprimi është marrë? A është riprodhuar mesazhi?
Kush tjetër e ka përdorur në media sociale?
A ngre shqetësime etike shpërndarja e mediave sociale?

Kjo kornizë është e inspiruar nga:

Diagrami "Hetimi i punimit të artit" (The "Interrogating the work of Art" diagram (Fig.2.4, faq.39), in (2014, 5th Edition), Pointon, M. History of Art: A Student's Handbook, London and New York: Routledge).

"Pyetje për të bërë për secilin element të një shembulli të çrregullimit të informacionit" ("Questions to ask about each element of an example of information disorder" (Fig. 7, faq. 28), (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. Si të mendohet për falsifikimet e thella (deepfake) dhe teknologjitë e reja të manipulimit

Shkruan: Sem Gregori

Sem Gregori *(Sam Gregory) është drejtor programi i WITNESS (Dëshmitar - www.witness.org), që i ndihmon njerëzit të përdorin videon dhe teknologjinë për të luftuar për të drejtat e njeriut. Një teknolog, avokues i vlerësuar dhe fitues i çmimeve, ai është ekspert i formave të reja të misinformatave (informatave të gabuara) dhe dezinformatave të nxitura/bëra nga IA (inteligjenca artificiale) dhe e udhëheq punën rreth mundësive dhe kërcënimeve të shfaqura ndaj aktivizmit dhe gazetarisë. Ai është gjithashtu bashkëkryetar i grupit të ekspertëve të Partneritetit për IA të fokusuar në IA dhe media.*

Në verën e vitit 2018, Profesori Sivei Lyi, një studiues kryesor i "deepfakes" (falsifikimeve të thella) me bazë në Universitetin e Albani (University of Albany), publikoi një studim që tregonte se video personat e "deepfake" nuk lëviznin qepallat e syve me të njëjtin ritëm si njerëzit e vërtetë. Për këtë pretendim u raportua së shpejti nga Fast Company, New Scientist, Gizmodo, CBS News dhe të tjerë, duke bërë që shumë njerëz të mendonin se tani kishin një mënyrë të fuqishme për të dalluar një deepfake.

Megjithatë, brenda disa javësh nga publikimi i punimit të tij, studiuesi pranoi video që tregonin një person deepfake që lëvizte qepallat e syve si një njeri. Që sot, kjo këshillë nuk është e dobishme apo e saktë. Ishte thembra e Akilit e një algoritmi të krijimit të falsifikime të thella në atë moment, bazuar në të dhënat e trajnimit që po përdoreshin. Por brenda disa muajsh, kjo nuk ishte më e vlefshme.

Kjo ilustron një të vërtetë kyçe rreth zbulimit dhe verifikimit të deepfake-ve: Qasjet teknike janë të dobishme deri në momentin kur teknikat e mediave sintetike do të përshtaten në mënyrë të pashmangshme me to. Një sistem i përsosur zbulimi i falsifikimeve të thella nuk do të ekzistojë kurrë.

Pra, si duhet të verifikojnë gazetarët falsifikimet e thella dhe format e tjera të mediave sintetike?

Hapi i parë është të kuptoni natyrën "mace dhe mi" të kësaj pune si dhe të jeni të vetëdijshëm se si po evoluon teknologjia. Së dyti, gazetarët duhet të mësojnë dhe të zbatojnë teknikat dhe mjetet themelore të verifikimit për të hetuar nëse një përmbajtje është manipuluar me qëllim të keq ose është krijuar në mënyrë sintetike. Të zbatueshme janë të gjitha qasjet për verifikimin e imazheve dhe videove të detajuara në Doracakun e parë të verifikimit, si dhe në resurset e First Draft në lidhje me verifikimin vizual. Më në fund, gazetarët duhet të kuptojnë se tashmë jemi në një mjedis ku pohimi i rremë se diçka është deepfake është gjithnjë e më i zakonshëm. Kjo do të thotë se aftësia për të verifikuar autenticitetin e një fotoje ose videoje është po aq e rëndësishme sa të dëshmosh se ajo është manipuluar.

Ky kapitull flet më gjerësisht për këto qasje thelbësore për verifikimin e falsifikimeve të thella (deepfake), por së pari është e rëndësishme të keni një kuptim bazik mbi falsifikimin e thellë dhe mediat sintetike.

Çfarë janë deepfakes dhe mediat sintetike?

Deepfakes (falsifikimet e thella) janë forma të reja të manipulimit audiovizual që i lejojnë njerëzit të krijojnë simulime reale të fytyrës, zërit ose veprimeve të dikujt. Ato u mundësojnë njerëzve të bëjnë të duket sikur dikush ka thënë ose ka bërë diçka që ata nuk e kanë bërë. Ato po bëhen më të lehta për t'u bërë, duke kërkuar më pak imazhe burimore për t'i ndërtuar ato, dhe po komercializohen gjithnjë e më shumë. Aktualisht, falsifikimet e thella ndikojnë në masë të madhe tek gratë, sepse përdoren për të krijuar imazhe dhe video seksuale pa pajtim (jokonsensuale) me fytyrën e një personi të caktuar. Por ekziston frika se falsifikimet e thella do të kenë një ndikim më të gjerë në shoqëri dhe në proceset e mbledhjes dhe verifikimit të lajmeve.

Falsifikimet e thella janë vetëm një zhvillim brenda një familjeje teknikash të mundësuara nga inteligjenca artificiale (IA) për gjenerimin e mediave sintetike. Ky grup mjetesh dhe teknikash mundëson krijimin e paraqitjeve realiste të njerëzve që bëjnë ose thonë gjëra që nuk i kanë bërë kurrë, krijimi realist i njerëzve/objekteve që nuk kanë ekzistuar kurrë, ose i ngjarjeve që nuk kanë ndodhur kurrë.

Teknologjia e mediave sintetike aktualisht i mundëson këto forma manipulimi:

- Të shtohen dhe hiqen objekte brenda një videoje.
- Të ndryshohen kushtet e sfondit në një video. Për shembull, ndryshimi i motit për ta bërë një video të xhiruar në verë të duket sikur është xhiruar në dimër.
- Të simulohet dhe kontrollohet një paraqitje realiste video e buzëve, shprehjeve të fytyrës ose lëvizjes së trupit të një individi të caktuar. Megjithëse diskutimi i falsifikimeve të thella në përgjithësi përqendrohet te fytyrat, teknika të ngjashme po aplikohen për lëvizjet e të gjithë trupit, ose pjesë të veçanta të fytyrës.
- Të gjenerohet një simulim realist i zërit të një personi specifik.
- Të modifikohet një zë ekzistues me një "lëkurë zëri" (voice skin) të një gjinie tjetër, ose të një personi specifik.
- Të krijohet një foto realiste, por tërësisht false e një personi që nuk ekziston. E njëjta teknikë mund të aplikohet edhe në mënyrë më pak problematike për të krijuar hamburger të rremë, mace, etj.
- Të transferohet një fytyrë reale nga një person tek tjetri, e njohur ndryshe si falsifikim i thellë (deepfake).

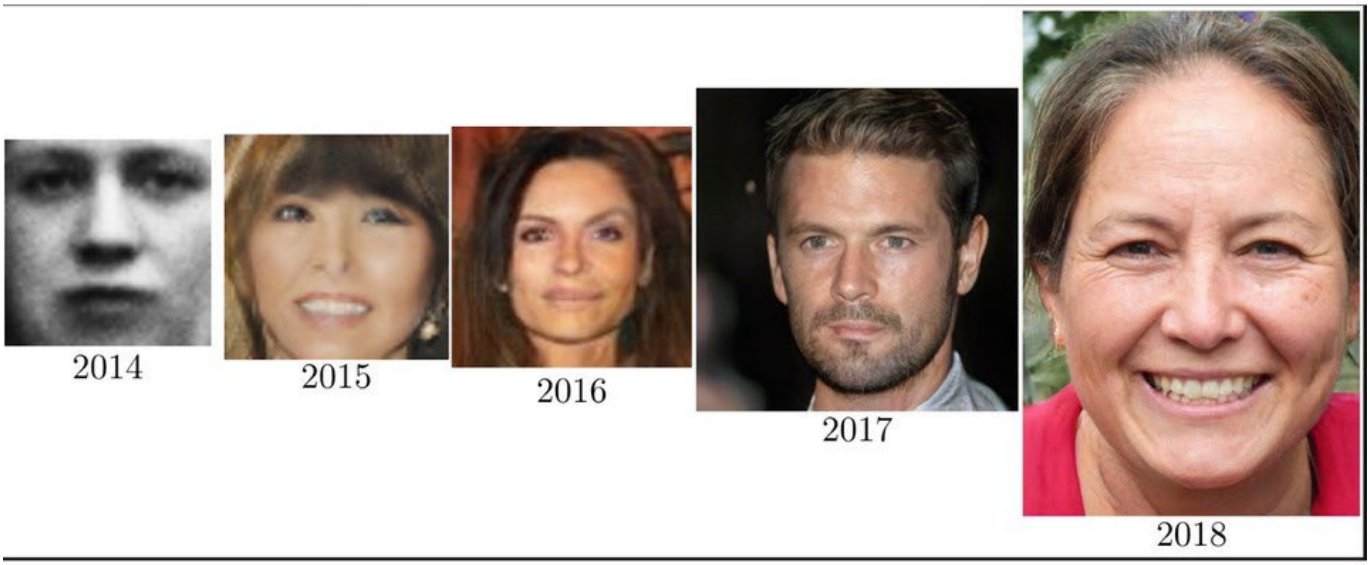
Këto teknika kryesisht, por jo ekskluzivisht, mbështeten në një formë të inteligjencës artificiale të njohur si "mësim i thellë" (deep learning) dhe ato që quhen Rrjetet Gjenerative Kundërshtare, ose GAN (Generative Adversarial Networks).

Për të gjeneruar një artikull me përmbajtje mediatike sintetike, filloni duke mbledhur imazhe ose video burimore të personit ose sendit që dëshironi të falsifikoni. Një GAN zhvillon falsifikimet – qofshin simulime video të një personi real ose shkëmbim fytyrash – duke përdorur dy rrjete. Një rrjet gjeneron rikrijime të besueshme të imazheve burimore, ndërsa rrjeti i dytë punon për të zbuluar këto falsifikime. Këto të dhëna zbulimi i kthehen rrjetit të angazhuar në krijimin e falsifikimeve, duke mundësuar përmirësimin e tij.

Nga fundi i vitit 2019, shumë nga këto teknika - veçanërisht krijimi i falsifikimeve të thella - vazhdojnë të kërkojnë fuqi të konsiderueshme kompjuteristike, një kuptim se si të akordoni modelin tuaj dhe shpesh edhe CGI (imazhe të krijuara nga kompjuteri – computer generated images) të rëndësishme post-produksioni për të përmirësuar rezultatin përfundimtar. Megjithatë, edhe me kufizimet aktuale, njerëzit tashmë po mashtrohen nga media të simuluara. Si shembull, hulumtimi nga projekti FaceForensics++ tregoi se njerëzit nuk mund të zbulonin me besueshmëri format aktuale të modifikimit të lëvizjes së buzëve, të cilat përdoren për të përshtatur gojën e dikujt me një pjesë të re audio. Kjo do të thotë që njerëzit, në thelb, nuk janë të pajisur për të zbuluar manipulimet e mediave sintetike.

Duhet gjithashtu të theksohet se audio sinteza po përparon më shpejt se sa pritej dhe po bëhet e disponueshme në treg. Për shembull, Google Cloud Text-to-Speech API ju mundëson të merrni një pjesë teksti dhe ta konvertoni atë në audio me një zë njerëzor që tingëllon sikur është real. Hulumtimet e fundit janë fokusuar gjithashtu në mundësinë e bërjes së tekstit për editimet e kombinuara të videos/audios në një video interviste.

Për më tepër, të gjitha tendencat teknike dhe ato të komercializimit tregojnë se do të vazhdojë të bëhet më e lehtë dhe më e lirë për të bërë media sintetike bindëse. Për shembull, imazhi i mëposhtëm tregon se sa shpejt ka avancuar teknologjia e gjenerimit të fytyrës.



Credit: EFF

Për shkak të natyrës "macja dhe miu" të këtyre rrjeteve, ato përmirësohen me kalimin e kohës derisa të dhënat mbi falsifikimet e suksesshme dhe zbulimin e suksesshëm ushqehen nëpërmjet tyre. Kjo kërkon kujdes të fortë në lidhje me efektivitetin e metodave të zbulimit.

Peizazhi aktual i falsifikimeve të thella dhe mediave sintetike

Falsifikimet e thella dhe mediat sintetike, nuk janë ende të përhapura gjerësisht jashtë imazheve seksuale jokonsensuale. Raporti i DeepTrace Lab mbi mbizotërimin e tyre që nga shtatori 2019 tregon se mbi 95% e falsifikimeve të thella ishin të këtij lloji, duke përfshirë ose të persona të famshëm, aktore pornografike ose njerëz të zakonshëm. Për më tepër, njerëzit kanë filluar të sfidojnë përmbajtjen reale, duke e hedhur poshtë atë si një falsifikim të thellë.

Në punëtoritë e udhëhequra nga WITNESS, i shqyrtuam vektorët e mundshëm të kërcënimit me një sërë pjesëmarrësish të shoqërisë civile, duke përfshirë media nga komunitetet (grassroot), gazetarë profesionistë dhe kontrollues të fakteve, si dhe studiues të misinformatave (informatave të gabuara) dhe dezinformatave dhe specialistë të OSINT. Ata u dhanë përparësi fushave ku format e reja të manipulimit mund të zgjerojnë kërcënimet ekzistuese, të prezantojnë kërcënime të reja, madje edhe të ndryshojnë kërcënimet ekzistuese ose të përforcojnë kërcënime të tjera. Ata identifikuan kërcënime për gazetarët, kontrolluesit e fakteve dhe hulumtuesit e burimeve të hapura, dhe sulme të mundshme ndaj proceseve të tyre. Ata gjithashtu theksuan sfidat rreth pohimit "është një falsifikim i thellë" si një kushëri retorik i "është lajm i rremë".

Në të gjitha kontekstet, ata vunë në dukje rëndësinë e shikimit të falsifikimit të thellë në kontekstin e qasjeve ekzistuese për kontrollimin dhe verifikimin e fakteve. Falsifikimet e thella dhe mediat sintetike do të integrohen në fushatat ekzistuese të konspiracionit dhe dezinformimit, duke u mbështetur në taktikat (dhe përgjigjet) në zhvillim në atë zonë, thanë ata.

Këtu janë disa kërcënime specifike që i theksuan:

- Gazetarëve dhe aktivistëve qytetarë do t'u sulmohet reputacioni dhe besueshmëria, duke u mbështetur në format ekzistuese të ngacmimit dhe dhunës onlajn që shënjestrojnë kryesisht gratë dhe pakicat. Një numër sulmesh duke përdorur video të modifikuara veçmë janë bërë ndaj grave gazetare, si në rastin e gazetares së shquar indiane Rana Ayyub.
- Figurat publike do të përballen me imazhe seksuale jokonsensuale dhe dhunë në bazë gjinore, si dhe me përdorime të tjera të të ashtuquajturve doppelgangers (njerëz që duken shumë ngjashëm me një person tjetër) të besueshëm. Politikanët lokal mund të jenë veçanërisht të cenueshëm, pasi kanë imazhe të shumta, por kanë pak strukturë institucionale rreth tyre si politikanët e nivelit kombëtar për t'u ndihmuar në mbrojtjen kundër një sulmi sintetik mediatik. Ata shpesh janë gjithashtu burime kyçe në mbulimin e lajmeve që rritet si flluskë nga niveli lokal në atë kombëtar.
- Përvetësimi i markave (brendeve) të njohura me modifikim të falsifikuar në video ose mënyra të tjera në të cilat një brend lajmesh, qeverie, korporate ose OJQ-je mund t'i bashkëngjitet në mënyrë të rreme një përmbajtjeje.
- Përpjekjet për të vendosur përmbajtje të krijuara nga përdoruesit që janë të manipuluara në ciklin e lajmeve, të kombinuara me teknika të tjera, si hakimi i burimeve ose shpërndarja e përmbajtjes së manipuluar deri te gazetarët në momente kyçe. Zakonisht, qëllimi është të nxiten gazetarët që të propagandojnë përmbajtjen.
- Përdorimi i dobësive të procesit të mbledhjes/raportimit të lajmeve, si transmetimet nga terreni me një kamerë të vetme (siç është vërejtur nga ekipi i Reuters UGC) dhe mbledhja e materialit në kontekste të vështira për t'u verifikuar si zona lufte ose vende të tjera.
- Ndërsa falsifikimet e thella bëhen më të zakonshme dhe më të lehta për t'u bërë në vëllim, ato do të kontribuojnë në tubë zjarri të të pavërtetave që vërshojnë verifikimin e mediave dhe agjencitë e verifikimit të fakteve me përmbajtje që duhet të verifikohen ose përgënjeshtrohen. Kjo mund t'i mbingarkojë dhe shpërqendrojë ata.
- Presioni do të jetë mbi organizatat që mbledhin dhe verifikojnë lajme për të dëshmuar se diçka është e vërtetë, si dhe për të dhënë prova se diçka nuk është e falsifikuar. Ata që janë në pushtet do të kenë mundësinë të përdorin mohim të besueshëm të ndonjë përmbajtjeje duke deklaruar se ajo është bërë me falsifikim të thellë.

Pikënisja për të verifikuar falsifikimet e thella

Duke pasur parasysh natyrën e forenzikës mediatike dhe teknologjive të reja të falsifikimeve të thella, duhet të pranojmë se mungesa e provave se diçka është e ndryshuar nuk do të jetë provë përfundimtare se media nuk është ndryshuar.

Gazetarët dhe hetuesit duhet të krijojnë një mentalitet të skepticizmit të matur rreth fotove, videove dhe audiove. Ata duhet të supozojnë se këto forma të medias do të sfidohen më shpesh përderisa njohuritë dhe frika nga falsifikimet e thella rritet. Është gjithashtu thelbësore të zhvillohet një njohje e fuqishme me mjetet e forenzikës mediatike.

Duke pasur këtë ndërmend, një qasje për të analizuar dhe verifikuar falsifikimet e thella dhe manipulimin e mediave sintetike duhet të përfshijë:

1. Rishikimi i përmbajtjes për defekte ose shtrembërime treguese që burojnë nga media sintetike.
2. Zbatimi i qasjeve ekzistuese të verifikimit dhe forenzikës për videot.
3. Përdorimi i qasjeve të reja të bazuara në IA dhe qasjeve të reja të forenzikës kur janë të disponueshme.

Rishikimi për defekte ose shtrembërime të dukshme

Kjo është qasja më pak e fuqishme për identifikimin e falsifikimeve të thella dhe modifikimeve të tjera të mediave sintetike, veçanërisht duke pasur parasysh natyrën evoluese të teknologjisë. Thënë kështu, deepfake-t e bëra keq ose përmbajtja sintetike mund të paraqesin disa dëshmi të gabimeve të dukshme. Gjërat për t'u kërkuar në një falsifikim të thellë përfshijnë:

- Shtrembërimet e mundshme në ballë/vijë flokësh ose kur fytyra lëviz përtej një hapësire të caktuar lëvizjeje.
- Mungesa e detajeve në dhëmbë
- Lëkurë tepër e lëmuar
- Mungesa e lëvizjes së qepallave të syve
- Një folës statik pa ndonjë lëvizje të vërtetë të kokës ose gamë të shprehjeve të fytyrës
- Defektet kur një person kthehet nga anfasi në profil (përballë dhe anësh)

Disa nga këto defekte aktualisht kanë më shumë gjasa të jenë të dukshme në një analizë fre-jm-pas-frejmi, kështu që nxjerrja e një sërë të frejmave për t'u rishikuar individualisht mund të ndihmojë. Ky nuk do të jetë rasti me defektet e lëvizjes ballore-anësore (anfas-profil) - këto shihen më së miri në një sekuencë, kështu që duhet të bëni të dyja qasjet.

Zbatimi i qasjeve ekzistuese për verifikimit të videos

Ashtu si me format e tjera të manipulimit të medias dhe falsifikimeve të cekëta (shallowfakes), të tilla si video të keqkontekstualizuara ose të edituara/redaktuara (montuara), duhet ta bazoni qasjen tuaj në praktika të etabluara verifikimi. Praktikat ekzistuese të verifikimit OSINT janë ende relevante, dhe një pikënisje e mirë janë kapitujt dhe rastet e studimit në Doracakun e parë kushtuar verifikimit të imazheve dhe videove. Meqenëse shumica e falsifikimit të thellë ose modifikimeve aktualisht nuk janë sintetizuara plotësisht, por në vend të kësaj bazohen në bërjen e ndryshimeve në një video burimore, mund të përdorni frejmat nga një video për të kërkuar versione të tjera duke përdorur një kërkim të kundërt të imazhit. Mund të kontrolloni gjithashtu videon për të parë nëse peizazhi dhe pikat referuese (landmarks) përputhen me imazhet e të njëjtës vendndodhje në Pamjen e Rrugëve të Google (Google Street View).

Në mënyrë të ngjashme, qasjet e bazuara në të kuptuarit se si shpërndahet përmbajtja, nga kush dhe si, mund të zbulojnë informacione nëse duhet t'i besohet një imazhi ose videoje. Bazat e përcaktimit të burimit, datës, kohës dhe motivimit të një përmbajtjeje janë thelbësore për të përcaktuar nëse ajo dokumenton një ngjarje apo person real. (Për vendosjen bazike në këtë qasje, shihni këtë udhëzues të First Draft) Dhe, si gjithmonë, është thelbësore të kontaktoni personin ose njerëzit e paraqitur në video për të kërkuar koment dhe për të parë nëse ata mund të japin informacion konkret për të mbështetur ose hedhur poshtë autenticitetin e saj.

Mjete të reja po zhvillohen gjithashtu nga qeveria, shkencëtarët, platformat dhe laboratorët e inovacionit gazetaresk për të ndihmuar në zbulimin e mediave sintetike, dhe për të zgjeruar disponueshmërinë e mjeteve forenzike të medias. Në shumicën e rasteve, këto mjete duhet të shihen si sinjale për të plotësuar qasjen tuaj të verifikimit të bazuar në praktikat më të mira.

Mjetet si InVID dhe Forensically ndihmojnë me verifikimin e imazheve të bazuar në origjinë dhe analizën e kufizuar forenzike.

Mjetet falas në këtë fushë përfshijnë:

- FotoForensics: Një mjet forenzik imazhesh që përfshin kapacitetin për Analizën e shkallës së gabimeve (Error Level Analysis) për të parë se ku mund të jenë shtuar elementët e një imazhi.
- Forensically: Një grup mjetesh për detektimin e klonimit, analizën e shkallës së gabimit, meta të dhënat (meta-data) të imazhit dhe një sërë funksionesh të tjera.
- InVID: Një shtesë e shfletuesit të uebit që ju mundëson të copëtoni videot në frejma, të kryeni kërkimin e kundërt të imazheve nëpër motorë të shumtë kërkimi, të përmirësoni dhe të eksploroni frejmat dhe imazhet përmes një thjerrëze zmadhuese dhe të aplikoni filtra forenzike në imazhe statike.

- Reveal Image Verification Assistant: Një mjet me një sërë algoritmesh për zbulimin e manipulimit të imazhit, plus analizën e meta të dhënave, vendndodhjen gjeografike GPS, nxjerrjen e fotografive EXIF dhe integrimin me kërkimin e kundërt të imazhit nëpërmjet Google.
- Ghiro: Një mjet i forenzikës digjitale onlajn me burim të hapur.

Vini re se pothuajse të gjitha këto janë krijuar për verifikimin e imazheve, jo videove. Kjo është një dobësi në hapësirën e forenzikës së medias, kështu që për videot është ende e nevojshme të nxirren imazhe individuale për analizë, për të cilat mund të ndihmojë InVID. Këto mjete do të jenë më efektive me video të pakompresuara me rezolucion më të lartë, të cilave, për shembull, u janë hequr ose shtuar video objekte brenda tyre. Përdorshmëria e tyre do të ulet sa më shumë që një video të jetë e kompresuar, e ri-ruajtur ose e shpërndarë nëpër media të ndryshme sociale dhe platforma për shpërndarje të videove.

Nëse jeni duke kërkuar për mjete të reja të forenzikës të medias për t'u marrë me çështjet ekzistuese të forenzikës vizuale, si dhe eventualisht me falsifikime të thella, një opsion është të shikoni mjetet që po shpërndahen nga shkencëtarët. Një nga qendrat më të avancuara kërkimore në Universitetin e Napolit ofron qasje onlajn në kodin e tyre, ndër të tjera, për zbulimin e gjurmëve të kamerës (Noiseprint), zbulimin e copëzave të një imazhi të vendosura në tjetër – image splices (Splicebuster) dhe zbulimin e veprimeve copy-move dhe remove (kopjim-lëvizje dhe fshirje) në video.

Ndërsa media sintetike përparon, forma të reja manuale dhe automatike të forenzikës së medias do të përsosen dhe do të integrohen në mjetet ekzistuese të verifikimit të përdorura nga gazetarët dhe zbuluesit e fakteve, si dhe potencialisht në qasjet e bazuara në platforma. Është e rëndësishme që gazetarët të punojnë për të qëndruar të përditësuar mbi mjetet e disponueshme, duke mos u varur tej mase prej tyre.

Qasjet e reja të forenzikës mediatike të bazuara në IA

Që nga fillimi i vitit 2020, nuk ka asnjë mjet zbulimi të testuar, të disponueshëm në treg të bazuar në GAN. Por duhet të parashikojmë se disa do të hyjnë në treg për gazetarët ose si plug-in ose si mjete në platforma në vitin 2020. Për një studim aktual të gjendjes së fushës në forenzikën e medias, duke përfshirë këto mjete, duhet të lexoni 'Forenzika mediatike dhe Deepfake-t: Përmbledhje" (Media Forensics and Deepfakes: An overview) nga Luisa Verdoliva.

Këto mjete do të mbështeten në përgjithësi në të dhënat e trajnuara (shembuj) të mediave sintetike të bazuara në GAN, që më pas të jenë në gjendje ta përdorin këtë për të zbuluar shembuj të tjerë që prodhohen duke përdorur teknika të njëjta ose të ngjashme. Si një shembull, programet forenzike të medias si FaceForensics++ gjenerojnë falsifikime duke përdorur mjetet ekzistuese konsumuese të falsifikimit të thellë dhe më pas përdorin këto vëllime të mëdha imazhesh të rreme si të dhëna trajnimi për algoritmet që të kryejnë zbulimin e deepfake-ve. Kjo do të thotë se ato mund të mos jenë efektive në metodat dhe teknikat më të fundit të falsifikimit.

Këto mjete do të jenë shumë më të përshtatshme për zbulimin e mediave të gjeneruara nga GAN sesa teknikat aktuale të forenzikës mediatike. Ata gjithashtu do të plotësojnë forma të reja të mjeteve të forenzikës mediatike që merren më mirë me avancimet në sintezë. Megjithatë, ato nuk do të jenë të pagabueshme, duke pasur parasysh natyrën kundërshtare të mënyrës se si media sintetike evoluon. Një pikë kyçe është se çdo tregues i sintezës duhet të kontrollohet dyfish dhe të vërtetohet me qasje të tjera verifikimi.

Falsifikimet e thella dhe media sintetike po evoluojnë me shpejtësi dhe teknologjitë po bëhen gjerësisht të disponueshme, të komercializuara dhe të lehta për t'u përdorur. Ato kanë nevojë për më pak përmbajtje burimore për të krijuar një falsifikim sesa mund të prisni. Ndërsa teknologjitë e reja për zbulim shfaqen dhe integrohen në platforma dhe në mjetet e gazetarëve/të krijuara përmes OSINT, mënyra më e mirë për t'iu qasur verifikimit është përdorimi i qasjeve ekzistuese për imazhe/video dhe plotësimi i tyre me mjete forenzike që mund të zbulojnë manipulimin e imazhit. T'i besosh syrit të njeriut nuk është një strategji e fuqishme!

7. Monitorimi dhe raportimi brenda aplikacioneve të grupeve dhe mesazheve të mbyllura

Shkruan: Kler Uordëll

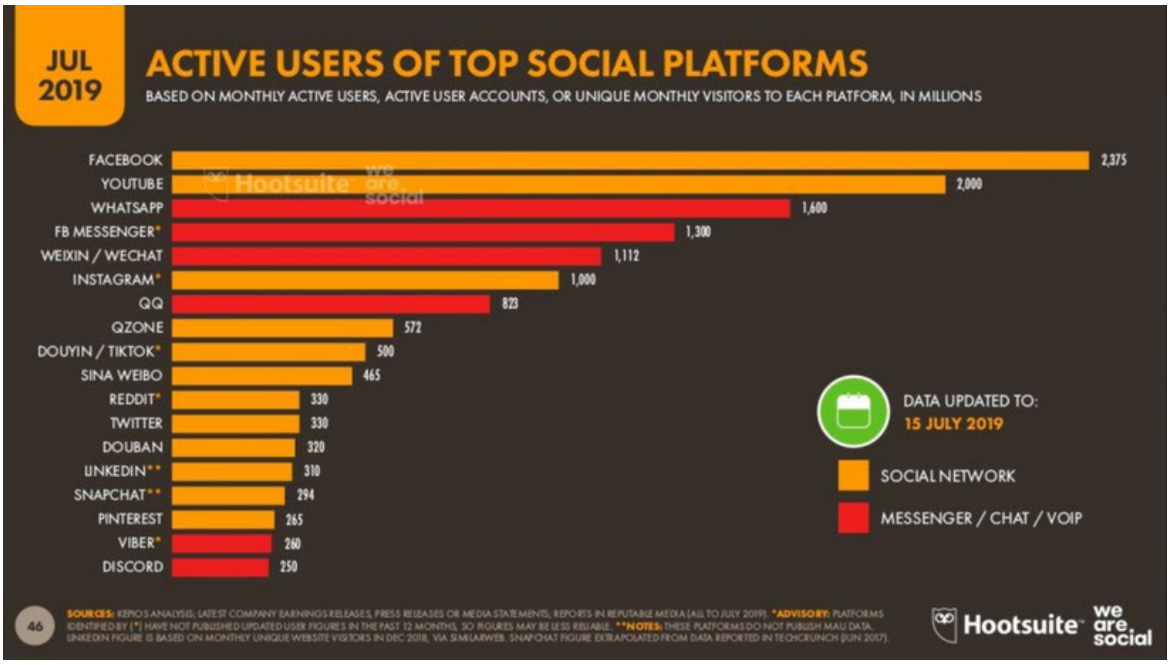
Kler Uordëll *(Claire Wardle) e udhëheq drejtimin strategjik dhe kërkimin për First Draft, organizatë jofitimprurëse globale që mbështet gazetarët, shkencëtarët dhe teknologët që punojnë për të adresuar sfidat në lidhje me besimin dhe të vërtetën në epokën digjitale. Ajo ka qenë bursiste e Qendrës Shorenstein për Media, Politikë dhe Politika Publike në Shkollën Kennedy të Harvardit, Drejtoreshë e kërkimeve në Qendrën Tow për Gazetari Digjitale në Shkollën Diplomike të Gazetarisë të Universitetit Columbia dhe drejtuese e mediave sociale për UNHCR, Agjencinë e Kombeve të Bashkuara për Refugjatë.*

Në mars të vitit 2019, Mark Zakerbergu foli mbi "lëvizjen drejt privatësisë" ("pivot to privacy") të Facebookut, që do të thoshte se kompania ishte duke i theksuar grupet e Facebookut, dhe si njohje se njerëzit tërhiqeshin gjithnjë e më shumë në komunikimin me numër më të vogël të njerëzve në hapësira private. Gjatë viteve të fundit, rëndësia e grupeve të vogla për komunikim-in social është bërë e qartë te ne që punojmë në këtë hapësirë.

Në këtë kapitull, do t'i shpjegoj platformat dhe aplikacionet e ndryshme, do të flas në lidhje me sfidat e monitorimit të këtyre hapësirave, dhe do të përfundoj me një diskutim për etikës e bërjes së këtij lloji të punës.

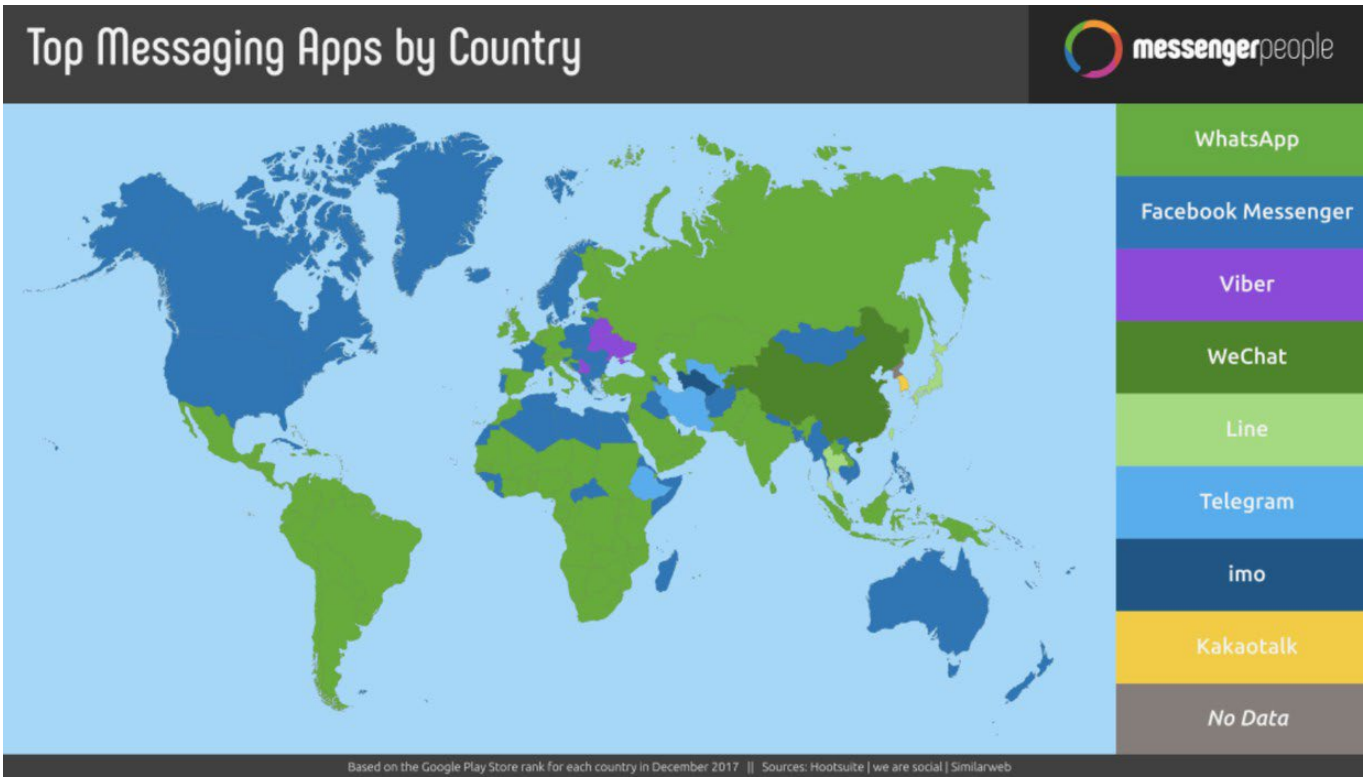
Platforma dhe aplikacione të ndryshme

Kërkime te fundit nga We Are Social (Ne jemi social), tregojnë dominimin e vazhdueshëm të Facebook-ut edhe YouTube-it, por tre platformat më të popullarizuara në vazhdim janë: Uatsapi (WhatsApp), Mesenxheri i Facebookut (FB Messenger), dhe UiÇati (WeChat).



Në shumë rajone anembanë botës, aplikacionet e bisedave janë burimi dominues i lajmeve për shumë konsumatorë, veçanërisht WhatsApp-i, për shembull, në Brazil, Indi, dhe Spanjë.

Sigurisht, WhatsApp dhe FB Messenger janë të popullarizuar globalisht, por në disa shtete të caktuara, alternativat janë dominuese. Për shembull, në Iran është Telegrami ,Lajni (Line) në Japoni, KakaoTalk në Korenë e Jugut, dhe Uiçati në Kinë.



Të gjitha këto faqe kanë ndryshime të vogla në funksionalitet, sa i përket enkriptimit, veçorive të grupit ose transmetimit dhe opsioneve shtesë, si mundësitë e tregtisë brenda aplikacionit,.

Grupet e mbyllura në Facebook

Ekzistojnë tre lloje të grupeve të Facebookut: të hapura, të mbyllura dhe të fshehura.

- Grupet e hapura mund të gjenden në motorin e kërkimit dhe çdokush mund të bashkohet.
- Grupet e mbyllura mund të gjenden në motorin e kërkimit për duhet të aplikoni për t'u bashkuar.
- Grupet e fshehura nuk mund të gjinden në motorin e kërkimit dhe duhet të jeni të ftuar për t'u bashkuar.

Gjithnjë e më shumë, njerëzit po mblidhen në grupet e Facebookut, pjesërisht nga arsyeja që ata po shtyhen nga algoritmi i Facebookut, por edhe sepse njerëzit janë duke zgjedhur të shpenzojnë kohë me njerëzit që veçmë i njohin, ose me njerëzit me të cilët ndajnë perspektivë apo interes të përbashkët.

Discord (Diskord)

Sipas Statista-s, në korrik të 2019-tës, Discord-i ka pasur 250 milionë përdorues aktivë (për krahasim, Snap-i ka pasur 294 milionë, Viber-i ka pasur 260 milionë dhe Telegrami ka pasur 200 milionë). Discord-i është i popullarizuar brenda komunitetit të gejmerëve (ata që luajnë lojëra video), por në vitet e fundit, është bërë i njohur edhe si faqe ku njerëzit mund të mblidhen në "serverë" (një formë e grupit në Discord) për të koordinuar fushata të dezinformatave.

Një aspekt i Discord-it dhe disa grupeve të fshehura të Facebook-ut është që do të pyeteni disa pyetje para se të pranoheni në atë grup. Këto pyetje mund të jenë në lidhje me profesionin tuaj, përkatësinë tuaj fetare, qëndrimet tuaja politike ose qëndrimet tuaja në lidhje me ndonjë çështje të caktuar sociale.

Enkriptimi, grupet dhe kanalet

Një arsye që këto platforma dhe aplikacione janë bërë kaq të popullarizuara është se ato ofrojnë nivele të ndryshme të enkriptimit. WhatsApp-i dhe Viber-i janë momentalisht më të sigurtat, që ofrojnë end-to-end enkriptim (nga të dyja anët e komunikimit). Të tjerët, sikur Telegrami, FB Messenger-i dhe Lajni (Line), ofrojnë enkriptim vetëm nëse e kyçni.

Disa aplikacione kanë grupe ose kanale ku i informacioni shpërndahet te një numër i madh i njerëzve. Grupi më i madh i WhatsApp mund t'i mbajë 256 njerëz. Grupet e FB Messenger mbajnë 250. Në Telegram, një grup mund të jetë privat apo publikisht i kërkueshëm, dhe mund t'i mbajë 200 persona. Menjëherë pasi ta arrijnë atë numër mund të konvertohen në super-grup ku mund të kyçen deri në 75 000 njerëz . Telegrami po ashtu ka kanale, dhe mundësi transmetimi përbrenda aplikacionit. Mund të abonoheni në një kanal dhe të shihni se çfarë është duke u publikuar atje, por ju nuk mund ta publikoni përmbajtjen tuaj si përgjigje.

Monitorim i vazhdueshëm

Nuk ka dyshim se dezinformata qarkullon në aplikacionet e mbyllura të mesazheve. Është e vështirë të vlerësohet në mënyrë të pavarur nëse ka më shumë dezinformata në këto platforma sesa në faqet e mediave sociale, sepse nuk ka asnjë mënyrë për të parë se çfarë po shpërndahet. Por, e dimë se është një problem, siç na kanë treguar rastet e profilit të lartë nga India, Franca dhe Indonezia. Por edhe në SHBA, gjatë të shtënave në El Paso dhe Dejton në gusht të vitit 2019, kishte shembuj të thashethemeve dhe të pavërtetave që qarkullonin në Telegram dhe FB Messenger.

Pyetja është nëse gazetarët, studiuesit, kontrolluesit e fakteve, punonjësit e shëndetësisë dhe punonjësit humanitarë duhet të jenë në këto grupe të mbyllura për të monitoruar dezinformatat. Nëse ata duhet të jenë në këto grupe, si duhet ta bëjnë punën e tyre në një mënyrë që është etike dhe i mban ata të sigurt?

Edhe pse ka sfida të rëndësishme për të bërë këtë punë, kjo është e mundur. Megjithatë, mbani mend se shumë njerëz që përdorin këto aplikacione e bëjnë këtë në mënyrë specifike që të mos monitorohen. Ata i përdorin ato sepse janë të koduara (enkriptuara). Ata presin një nivel të caktuar privatësie. Kjo duhet të jetë thelbësore për këdo që punon në këto hapësira. Edhe pse mund të bashkoheni dhe të monitoroni këto hapësira, është thelbësore të jeni të vetëdijshëm për përgjegjësinë që keni ndaj pjesëmarrësve në këto grupe, të cilët shpesh nuk e kuptojnë se çfarë është e mundur.

Teknikat për kërkim

Kërkimi për këto grupe mund të jetë i vështire, sepse ka protokolle të ndryshme për secilin. Për grupet e Facebookut, mund të kërkoni për tema brenda motorit të kërkimit në Facebook dhe filtrimit sipas grupit. Nëse doni të përdorni operatorë më të sofistikuar Boolean, kërkoni në Google duke përdorur fjalët tuaja kyçe dhe pastaj shtoni "site:facebook/groups".

Për Telegramin, mund të kërkoni në aplikacion nëse keni telefon Android, por jo në qoftë se keni Ajfon. Ka desktop-aplikacione, si https://www.telegram-group.com/ Ngjashëm edhe për Discord, ka faqe si https://disboard.org/search

Vendimet rreth anëtarësimit dhe pjesëmarrjes

Siç u përmend, disa nga këto grupe do pyesin për ta siguruar kyçjen. Para se ta provoni këtë, duhet të flisni me redaktorin apo menaxherin tuaj se si t'u përgjigjeni këtyre pyetjeve. A do të jeni të sinqertë se kush jeni dhe pse jeni në grup? A ka ndonjë mënyrë për t'u anëtarësuar duke qëndruar qëllimisht i paqartë? Nëse jo, si mund ta justifikoni atë vendim për të fshehur identitetin tuaj (kjo mund të jetë e nevojshme nëse po i bashkoheni një grupi që mund të rrezikojë sigurinë tuaj nëse identifikoheni si gazetar). Nëse fitoni qasje, a do të kontribuoni në çfarëdo mënyre, apo thjesht do të "endeni" për të gjetur informacione që mund t'i konfirmoni diku tjetër?

Vendime për mbledhje automatike të përmbajtjeve nga grupet

Është e mundur të gjinden grupe të "hapura" duke kërkuar linqe që janë postuar në faqe tjera. Pastaj këto paraqiten në motorët e kërkimit. Dhe pastaj është e mundur të përdoren metodat kompjuterike për të mbledhur automatikisht përmbajtjet nga këto grupe. Hulumtuesit që monitoronin zgjedhjet në Brazil dhe Indi e kanë bërë këtë, dhe e di në mënyrë anekdotike për organizata të tjera që bëjnë punë të ngjashme.

Kjo teknikë lejon organizatat të monitorojnë njëherësh më shumë grupe të ndryshme, që përndryshe është shpesh e pamundur. Pika kyçe është që vetëm një përqindje e vogël e grupeve janë mund të gjenden në këtë mënyrë, dhe ato zakonisht qëllojnë të jenë grupe që medoemos dëshirojnë anëtarësim më të gjerë, kështu që nuk janë reprezentative për të gjitha grupet. Për mua po ashtu kjo ngre edhe çështje etike. Sidoqoftë, ka "guardrails" (binarë të rojës) që mund të përdoren për t'u mbrojtur të dhënat, duke mos ndarë me të tjerët dhe duke de-identifikuar mesazhet. Kemi nevojë për protokolle ndër-industriale për ta bërë këtë lloj pune.

Linja informimi (Tiplines)

Teknika tjetër është të vendosni një linjë informimi (tipline), ku inkurajoni publikun që t'ju dërgojë përmbajtje. Çelësi për një linjë informimi është të keni një thirrje të thjeshtë dhe të qartë për veprim dhe të shpjegoni se si synoni ta përdorni atë përmbajtje. A është thjesht për monitorimin e trendëve apo do t'u përgjigjeni atyre me përgënjeshtrim pasi të keni hulumtuar informatat që ju dërgohen?

Duke u kthyer te pyetjet etike, që kanë ndikim të madh në lidhje me punën me aplikacionet e mesazheve të mbyllura, është e rëndësishme që ju nuk jeni vetëm "duke e marrë" përmbajtjen, ose në fjalë tjera duke qenë ekstraktiv. Dhe nëse e lëmë etikën anash për një çast, i gjithë hulumtimi tregon që nëse audienca nuk di se si po përdoren informatat e tyre, ata me shumë gjasë do të ndalojnë të dërguarit. Njerëzit më shumë duan të ndihmojnë kur ndjejnë po trajtohen si partnerë.

Aspekti tjetër, sidoqoftë, është se sa lehtë është bëhet lojë me linjat e informimit duke dërguar përmbajtje mashtruese, ose nëse një individ apo grup i vogël dërgon përmbajtje të njëjtë që të duket problem më i madh sesa që është.

Etika e raportimit nga grupet e mbyllura për mesazhe

Pasi ta keni gjetur përmbajtjen, pyetja është se si të raportohet mbi të. A duhet të jeni transparent në lidhje me atë se si e keni gjetur? Si pjesë e udhëzimeve të tyre të komunitetit, shumë grupe kërkojnë që ajo që diskutohet në grup të mos shpërndahet më gjerë. Në qoftë se grupi është i mbushur me dezinformata, cili do të jetë ndikimi i raportimit tuaj për të? A mund ta vërtetoni atë që keni gjetur në grupe tjera apo në hapësira onlajn? Nëse raportoni, a mund ta rrezikoni sigurinë tuaj, ose atë të kolegëve ose familjes suaj? Mbani mend që kërcënimi ndaj gazetarëve dhe hulumtuesve (ose edhe më keq) është pjesë e mënyrës së veprimit për disa nga grupet më të errëta onlajn.

Përfundime

Raportimi nga dhe për aplikacionet e mesazheve dhe grupeve të mbyllura është përplot me sfida, mirëpo ato burime do të bëhen edhe më të rëndësishme si hapësira ku shpërndahet informacioni. Si hap i parë, mendoni mbi pyetjet e theksuara në këtë kapitull, flisni me kolegët dhe redaktorët tuaj, dhe nëse ju nuk keni udhëzime në redaksi në lidhje me këtë lloj të raportimit, filloni të punoni në për të krijuar disa. Nuk ka rregulla standarde për mënyrën se si ta bëni këtë. Kjo varet nga storia, platforma, reporteri dhe udhëzimet editoriale të redaksisë. Por është e rëndësishme që të gjitha detajet të merren në konsideratë para se të filloni me këtë lloj të raportimit.

7a. Rast studimi: Bolsonaro në spital

Shkruan: Serhio Lydke

Serhio Lydke *(Sergio Lüdtke) është gazetar dhe redaktor i Projeto Comprova, një koalicion i 24 organizatave mediatike që bashkëpunojnë për të hulumtuar thashethemet mbi politikat publike në Brazil.*

Në vitin 2018, Comprova shqyrtoi përmbajtjen e dyshimtë të shpërndarë në mediat sociale dhe aplikacionet e mesazheve në lidhje me zgjedhjet presidenciale në Brazil.

Më 6 shtator 2018, një muaj para zgjedhjeve presidenciale në Brazil, kandidati i të djathtës ekstreme Jair Bolsonaro mbajti një eveniment fushate në qendrën e Juiz de Fora, qytet me 560,000 banorë, 200 kilometra nga Rio de Zhaneiro.

U bë një javë qëkur Bolsonaro ishte bërë lider në sondazhet për raundin e parë të zgjedhjeve presidenciale të Brazilit. Ai mori pozitën e parë pasi që kandidatura e ish presidentit Luiz Inacio Lula da Silva, më parë lider i izoluar në sondazhe, mori ndalesë nga Gjykata e Lartë Zgjedhore.

Bolsonaro, megjithatë, po humbiste prej tre nga katër kandidatët më të afërt në sondazhe në simulimet e balotazhit.

Situata e Bolsonaros ishte brengosëse, pasi ai kishte vetëm dy blloqe ditore 9-sekondëshe në transmetimet elektorale pa pagesë në TV. Rregullat zgjedhore të Brazilit kërkojnë që radiot dhe stacionet televizive t'u japin kohë pa pagesë partive politike që t'i publikojnë propozimet e tyre. Kësaj radhe kjo ishte shpërndarë sipas numrit të ulëseve të fituara nga secila parti në zgjedhjet e fundit për Dhomën e Përfaqësuesve. Mungesa e ulëseve për Bolsonaron nënkuptonte shumë pak kohë transmetimi pa pagesë. Dhe, si rezultat i kësaj, ai u detyrua të mbështetet në përkrahësit e tij në rrjetet sociale dhe të bënte kontakte të drejtpërdrejta me votuesit në rrugë.

Në Juiz de Fora, sikur edhe në qytetet tjera që i vizitoi më parë, Bolsonaro mori pjesë në një marsh duke u mbajtur mbi supe nga përkrahësit e tij. Ai u tërhoq nga turma e admiruesve kur marshi papritmas u ndërpre. Në mes të turmës, një njeri zgjati dorën dhe e theri kandidatin. Thika la një plagë të thellë në barkun e Bolsonaros – dhe e hapi kutinë e Pandorës në rrjetet sociale.

U shpërndanë thashetheme dhe teori konspirative, disa prej tyre e akuzuan Adelio Bispo de Oliveira, njeriun që e theri Bolsonaron, për lidhje me ish-presidentin e partisë, Dilma Rousseff, që ishte e larguar nga zyra në 2016-tën. Foto të rreme shfaqën sulmuesin duke qëndruar afër Lulës (nofka e ish presidentes). Ajo që Bispo kishte lidhje me majtistët Partido Socialismo e Liberdade (PSOL), dhe refuzimi i avokatit tij të tregojë se kush po i paguante shpenzimet e tij, vetëm shërbeu për t'i ushqyer pretendimet konspirative.

Njëkohësisht, videot dhe mesazhet që u përpoqën të nënvlerësonin Bolsonaron fituan vëmendje në platformat e mediave sociale. Disa nga përmbajtjet malicioze pretenduan se therja ishte e inskenuar, se Bolsonaro realisht ka qenë në spital për ta trajtuar kancerin, dhe fotot që janë publikuar duke e treguar operacionin janë të falsifikuara.

Therja i dha Bolsonaros arsye të tërhiqet nga aktivitetet e fushatës, por i solli atij një pozicion më të mirë në sondazhe. (Në fund, kuptohet, Bolsonaro i fitoi zgjedhjet).

Më 19 shtator, afër dy javë pas sulmit, "Eleigoes sem Fake", një program grupor i monitorimit të WhatsApp-it i krijuar nga Universiteti i Minas Gerais, identifikoi një audio incizim që po qarkullonte. Audioja ishte shpërndarë nga 16 prej gati 300 grupeve të monitoruara nga projekti, disa prej të cilëve ishin përkrahës të Bolsonaros.

Po të njëjtën ditë, organizata jonë, Comprova, filloi të merrte, po ashtu përmes WhatsApp-it, kërkesa nga lexuesit për ta verifikuar integritetin e incizimit.

Në këtë audio, që ishte rreth një minutë e gjatë, një njeri i mllefosur, me zë që i përngjante Bolsonaros, fjalosej me dikë që pretendohej të ishte i biri, Eduardo, dhe ankohej në lidhje me mbajtjen e tij në spital. Në incizim, njeriu tha që ai nuk mundet më shumë ta përballojë "këtë teatër", duke sugjeruar se e gjitha kjo ishte një aktrim.

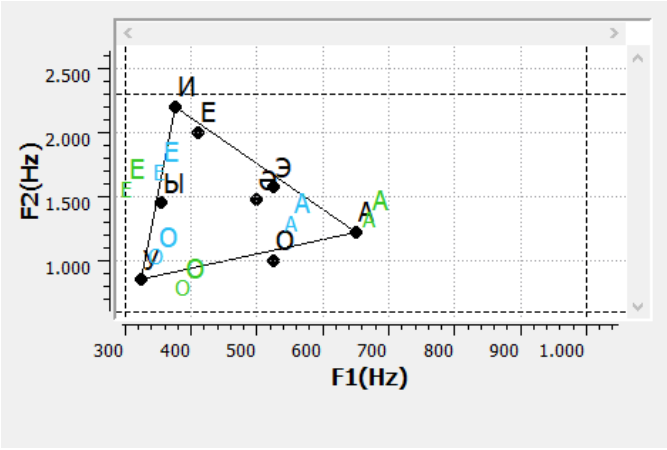
Atë ditë, Bolsonaro ishte ende pacient në njësinë e kujdesit gjysmë-intensiv në spitalin Albert Ajnshtajn në Sao Paulo. Raporti mjekësor thoshte që ai nuk kishte ethe, se merrte ushqim intravenoz dhe kishte rikuperuar funksionin e zorrëve.

Comprova nuk mund ta gjente burimin origjinal të incizimit. Audioja më së pari u shpërnda përmes WhatsApp-it në kohën kur fajlet mund të shpërndaheshin në deri 20 biseda. Kjo mundësoi që të shpërndahet rrufeshëm, dhe të depërtonte për kohë të shkurtë edhe në rrjetet tjera sociale. U bë e pamundur për ta gjurmuar burimin origjinal. (që atëherë WhatsApp ka kufizuar numrin e grupeve të cilave mund t'u ripërcillni (forvardoni) një mesazh).

Në pamundësi për të identifikuar autorin(ët) e incizimit, Comprova u fokusua në hulumtim më konvencional, dhe kërkoi ndihmë përmes një raporti ekspertësh nga Instituto Brasileiro de Perfcia (Instituti Brazilian i Mjekësisë Ligjore). Ekspertët e krahasuan incizimin me zërin të Bolsonaros nga një intervistë në prill të 2018-tës dhe ranë në përfundim që zëri i kandidatit nuk ishte zëri i personit në incizimin e shpërndarë në rrjetet sociale.

Ekspertët bënë një analizë kualitative të zërit, të të folurit dhe shënuesve (markerëve) gjuhësor të njeriut që foli në incizim. Pastaj, i krahasuan këta parametra në secilën mostër të zërit dhe të të folurit. Në këtë analizë, ata hulumtuan paternët (shabllonet) e zanoreve dhe bashkëtingëllorëve, ritmin e të folurit dhe shpejtësinë, paternët e intonacionit, kualitetin e zërit dhe shprehitë të prezantuara nga folësi, si dhe përdorimin e fjalëve specifike dhe rregullave gramatikore.

Për shembull, imazhi poshtë tregon një analizë frekuencash të "formantëve", emri i lartësive të prodhuara nga vibracionet e traktit vokal, zgavra ku filtrohet zëri i prodhuar në laring. Ajri brenda traktit të vokalit vibron në lartësi të ndryshme, varësisht nga madhësia dhe forma e hapjes. Imazhi tregon analizë frekuencash të formantëve duke përdorur zanoret "a", "e", dhe "o". Zanoret e gjelbra korrespondojnë me mostrën e audios që e siguruam nga WhatsApp, ndërsa zanoret e kaltra korrespondojnë me mostrat e marra nga një intervistë e dhënë e Bolsonaros disa ditë përpara sulmit mbi të.



Një analizë shtesë gjeti se folësi në audion e WhatsApp-it kishte një theks tipik nga zona rurale e shtetit të Sao Paulos. Por kjo nuk u paraqit në paternin (shabllonin) e të folurit të Bolsonaros. Dallimet në rezonancë, artikulim, shpejtësinë e të folurit dhe devijimin fonetik u detektuan në mostrat e krahasuara.

Comprova këshilloi një ekspert të dytë. Edhe ky profesionist po ashtu konkludoi se zëri në incizim dallonte nga i Bolsonaros për disa arsye. Ai tha që toni i zërit të tij paraqitej të ishte pak më akut nga ai i Bolsonaros. Ai vërejti që ritmi i të folurit ishte po ashtu më i shpejtë sesa një video tjetër e incizuar nga kandidati në spital.

Një element tjetër që përforcoi përfundimin se audioja ishte e rreme ishte kualiteti i dobët i incizimit. Sipas ekspertëve me përvojë, kjo ishte truk tipik i mashtrimit: zvogëlimi i rezolucionit të audiove, videove dhe fotove e bën analizën e tyre më të vështirë.

Sa i përket përgjigjes së Bolsonaros, djemtë e tij, Flavio dhe Karlos, postuan në mediat sociale duke thënë se audio ishte "lajm i rremë".

Nëse kjo audio do të bëhej virale sot, me siguri do të ishte më e vështirë të besohet se zëri ishte i Bolsonaros. Para zgjedhjeve, me vetëm 18 sekonda në ditë në televizion, dhe mungesa e tij nga debatet e fushatës për shkak të shtrimit në spital dhe mjekimit, zëri i presidentit të tashëm nuk ishte i njohur mirë. Kjo krijoi mundësi që një audio të rreme të mashtrojë shumë njerëz.

Sidoqoftë, pas më shumë se një viti, është ende e vështirë të kuptojmë se pse grupet në favor të Bolsonaros ose që bënin fushatë për kandidaturën e tij e shpërndanë audion, gjë që, nëse ishte dëshmuar se ishte autentike, do ta kishte shkatërruar kandidaturën e tij. Nuk do të mund ta dimë asnjëherë plotësisht se pse këto grupe e shpërndanë këtë përmbajtje me aq zell të madh. Pa marrë parasysh, kjo është një përforcim i fuqishëm i faktit që një përmbajtje, e cila bën një pretendim shpërthyes, do të shpërndahet rrufeshëm nëpër mediat sociale.

8. Hetimi i uebfaqeve

Shkruan: Kreg Silvermen

Kreg Silvermen *(Craig Silverman) është redaktor mediatik i BuzzFeed News, ku drejton ritmin global që mbulon platformat, keqinformimin onlajn dhe manipulimet mediatike. Ai më parë ka redaktuar "Doracakun e verifikimit" dhe "Doracakun e verifikimit për raportimin hulumtues", dhe është autor i "Gënjeshtrat, gënjeshtrat e mallkuara dhe përmbajtja virale: Si uebfaqet e lajmeve përhapin (dhe përgënjeshtrojnë) thashethemet në internet, pretendimet e paverifikuara dhe informatat e gabuara (misinformatat)."*

Uebfaqet përdoren nga ata që angazhohen në manipulimet mediatike për të fituar të ardhura, për të mbledhur e-maile dhe informacione të tjera personale, ose për të krijuar një fortifikim onlajn në ndonjë mënyrë. Gazetarët duhet të kuptojnë se si të hetojnë një prani në ueb dhe, kur është e mundur, ta lidhin atë me një operacion më të madh që mund të përfshijë llogari të mediave sociale, aplikacione, kompani ose subjekte të tjera.

Mos harroni se teksti, imazhet ose e gjithë faqja mund të zhduket me kalimin e kohës – veçanërisht pasi të filloni të kontaktoni njerëz dhe të bëni pyetje. Një praktikë më e mirë është të përdorni Wayback Machine për të ruajtur faqe të rëndësishme të uebfaqes që synoni si pjesë e rrjedhës suaj të punës. Nëse një faqe nuk do të ruhet siç duhet atje, përdorni një mjet tjetër si archive.today. Kjo siguron që ju të mund të vendosni linqe me faqet e arkivuara si provë të asaj që keni gjetur, dhe të shmangni linqe të drejtpërdrejta me një faqe që shpërndan informata të gabuara (misinformata) dhe dezinformata (Hunchly është një mjet i shkëlqyer me pagesë për të krijuar arkivin tuaj personal të uebfaqeve automatikisht deri sa punoni). Këto mjete arkivimi janë gjithashtu thelbësore për të hetuar se si është dukur një uebfaqe me kalimin e kohës. Rekomandoj gjithashtu instalimin e shtesës së shfletuesit Wayback Machine në mënyrë që të jetë e lehtë të arkivohen faqet dhe të shikohen versionet e mëparshme.

Një tjetër shtesë e dobishme e shfletuesve është Ghostery, e cila do t'ju tregojë gjurmuesit e pranishëm në një uebfaqe. Kjo ju ndihmon të identifikoni shpejt nëse një uebfaqe përdor Google Analytics dhe/ose ID të Google AdSense, gjë që do të ndihmojë me një nga teknikat e përshkruara më poshtë.

Ky kapitull do të vështrojë katër kategori që janë të nevojshme t'u analizuar kur hulumtoni një uebfaqe: përmbajtjen, kodin, analitikën, regjistrimin dhe elementët e lidhur.

Përmbajtja

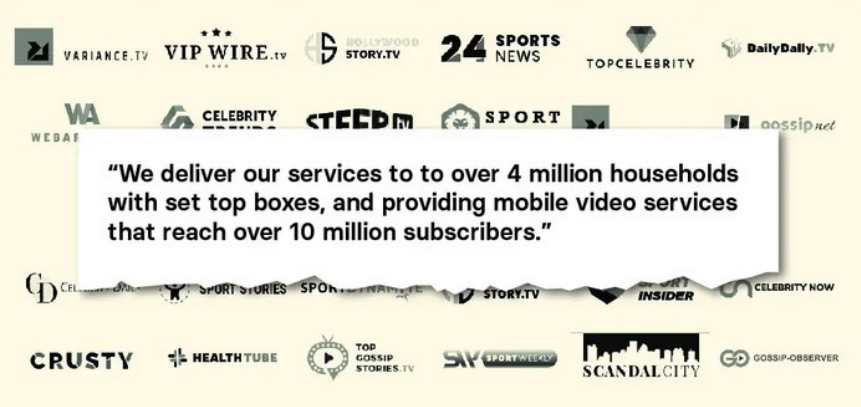
Shumica e uebfaqeve ju tregojnë të paktën diçka për atë se çfarë janë. Qoftë në një faqe të dedikuar "Rreth nesh" ose "Për ne" (About), një përshkrim në fund të faqes ose diku tjetër - ky është një vend i mirë për të filluar. Në të njëjtën kohë, mungesa e informacionit të qartë mund të jetë një tregues se faqja është krijuar me nxitim, ose po përpiqet të fshehë detaje rreth pronësisë dhe qëllimit të saj.

Së bashku me leximin e çdo teksti bazë "rreth nesh"(About), bëjeni një rishikim të plotë të përmbajtjes në uebfaqe, duke drejtuar sytë për të përcaktuar se kush e drejton atë, cili është qëllimi dhe nëse është pjesë e një rrjeti apo nisme më të madhe. Ja disa gjëra për të kërkuar:

- A e identifikon pronarin ose ndonjë entitet korporativ në faqen e saj "Rreth nesh"? Gjithashtu vini re nëse nuk ka një faqe "Rreth nesh".
- A liston një kompani ose një person në njoftim për të drejtat e autorit në fund të faqes kryesore ose ndonjë faqeje tjetër?
- A liston emra, adresa ose entitete korporative në politikën e privatësisë ose në termat dhe kushtet (terms and conditions)? A janë këto emra kompanish të ndryshëm nga ata që janë renditur në fund të faqes, në faqen "Rreth nesh" ose në vende të tjera në faqe?
- Nëse faqja publikon artikuj, vini re rreshtat e parë dhe nëse kanë lidhje të klikueshme. Nëse po, shikoni nëse ato çojnë në një faqe të autorit me më shumë informacion, si biografi ose linqe me llogaritë sociale të shkrimtarit.

- A përmban faqja llogari sociale të lidhura? Këto mund të jenë në formën e ikonave të vogla në krye, në fund ose në ndonjë anë të faqes kryesore, ose një "embed" që ju fton të pëlqeni faqen në Facebook, për shembull. Nëse faqja shfaq ikona për platforma të tilla si Facebook dhe Twitter, vendoseni miun mbi to dhe shikoni në pjesën e poshtme majtas të dritares së shfletuesit tuaj për të parë URL-në ku ato çojnë. Shpesh, një uebfaqe e krijuar me ngut nuk do të shqetësohet të plotësojë ID-të specifike të profilit social në shablonin (templejtin) e një faqe interneti. Në atë rast, thjesht do të shihni lidhjen të shfaqet si facebook.com/ pa një emër përdoruesi.
- A liston faqja ndonjë produkt, klient, dëshmi, apo njerëz ose kompani të tjera që mund të kenë një lidhje dhe që ia vlen të shikohen më tej?
- Sigurohuni që të gërmoni përtej faqes kryesore. Klikoni në të gjitha menytë kryesore dhe lëvizni poshtë deri në fund për të gjetur faqe të tjera që ia vlen të vizitohen.
- Një pjesë e rëndësishme e ekzaminimit të përmbajtjes është të shihet nëse është origjinale. A është kopjuar teksti nga faqja "Rreth nesh" ose ndonjë tekst tjetër i përgjithshëm nga diku tjetër? A po përhap faqja informacione të rreme ose keqorientuese, ose a po ndihmon në shtytjen e ndonjë agjende specifike?

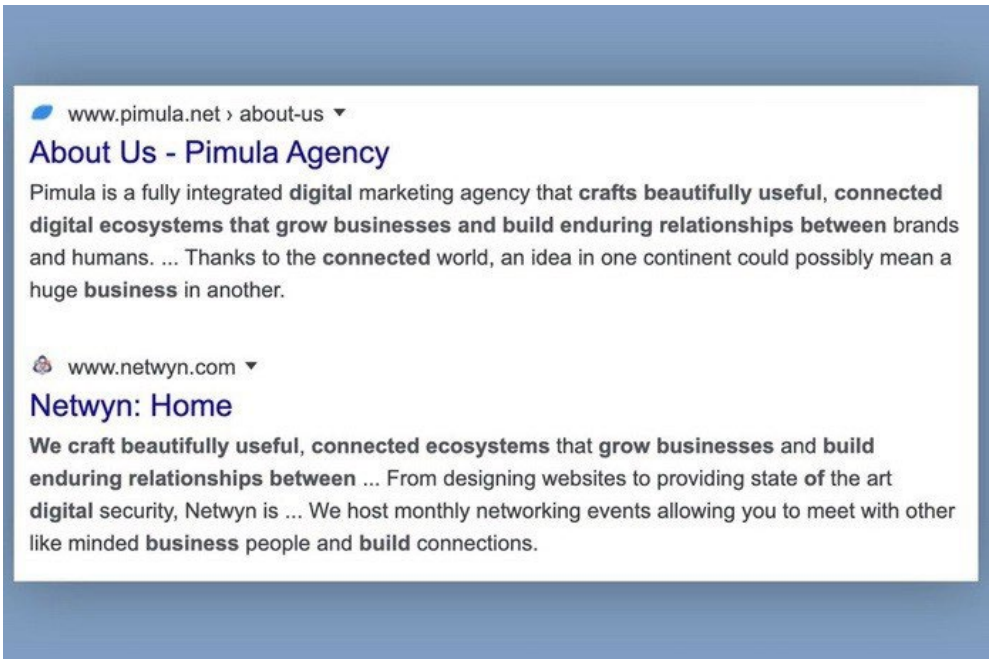
Në vitin 2018 hulumtova një skemë të madhe mashtrimi të reklamave digjitale që përfshinte aplikacione celulare dhe uebfaqe me përmbajtje, si dhe kompani guaska (shell companies), nëpunës të rremë dhe kompani false. Më në fund, gjeta më shumë se 35 uebfaqe të lidhura me skemën. Një mënyrë në të cilën identifikova shumë nga faqet ishte duke kopjuar tekstin në faqen "Rreth faqes" dhe duke e ngjitur atë në kutinë e kërkimit të Google. Menjëherë gjeta afër 20 faqe interneti me të njëjtin tekst:



Mashtruesit që drejtonin skemën krijuan gjithashtu uebfaqe për kompanitë e tyre parësore për t'i ndihmuar që të duken legjitime kur partnerët e mundshëm në rrjetet e reklamave vizitonin ato për të kryer kontrollimin e duhur. Një shembull për këtë ishte një kompani e quajtur Atoses. Faqja e saj kryesore listonte disa nëpunës me fotografi. Kërkimi i imazhit të kundërt në Yandex (kërkimi më i mirë i imazheve për fytyrat) zbuloi shpejt se disa prej tyre ishin stok imazhe (stock images – fotografi që veçmë ekzistojnë dhe gjenden në uebfaqe për blerje ose për përdorim pa pagesë të fotografive):

Atoses kishte gjithashtu këtë footer (tekst në fund të faqes së saj): “Ne krijojmë ekosisteme të bukura që janë të dobishme dhe të konektuara, të cilat rritin bizneset dhe ndërtojnë marrëdhënie të qëndrueshme midis mediave onlajn dhe përdoruesve.”

I njëjti tekst shfaqet në faqet e të paktën dy agjencive të marketingut:



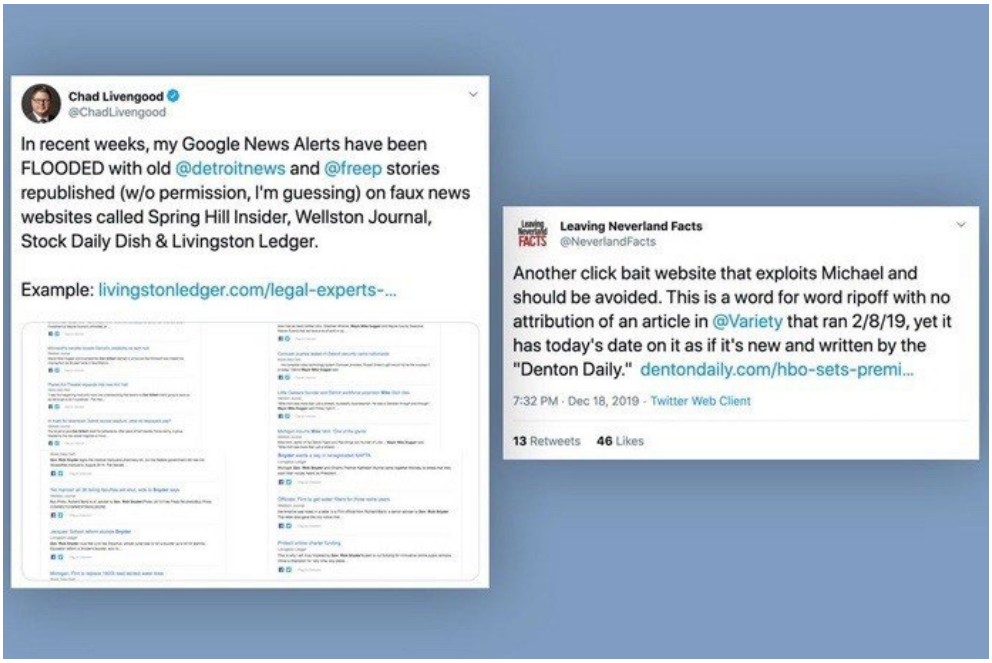
Nëse një kompani po përdor stok imazhe për punonjësit dhe tekst plagjiaturë në faqen e saj, e dini se ajo nuk është ajo që pretendon se është.

Është gjithashtu një ide e mirë të kopjoni dhe ngjitni tekstin nga artikujt në një faqe dhe t’i futni ato në Google ose në një motor tjetër kërkimi. Ndonjëherë, një faqe që pretendon se është burim lajmesh bën thjesht vetëm plagjiaturë të mediave të vërteta.

Në vitin 2019, hasa në një faqe të quajtur forbesbusinessinsider.com që dukej të ishte një faqe lajmesh që mbulonte industrinë e teknologjisë. Në realitet ajo bënte plagjiaturë masive të artikujve nga një shumëllojshmëri e gjerë mediash, duke përfshirë, që ishte qesharake, një artikull që shkrova për uebfaqet e rreme lokale.

Një hap tjetër bazik është të merrni URL-në e një faqeje dhe ta kërkoni atë në Google. Për shembull, “forbesbusinessinsider.com.” Kjo do t’ju japë një sens se sa nga faqet në internet janë indeksuar, dhe gjithashtu mund të sjellë shembuj të njerëzve të tjerë që raportojnë ose flasin diçka rreth faqes. Gjithashtu, mund të kontrolloni nëse faqja është e listuar në Google News duke hapur faqen kryesore të Google News dhe duke futur “forbesbusinessinsider.com” në kutinë e kërkimit.

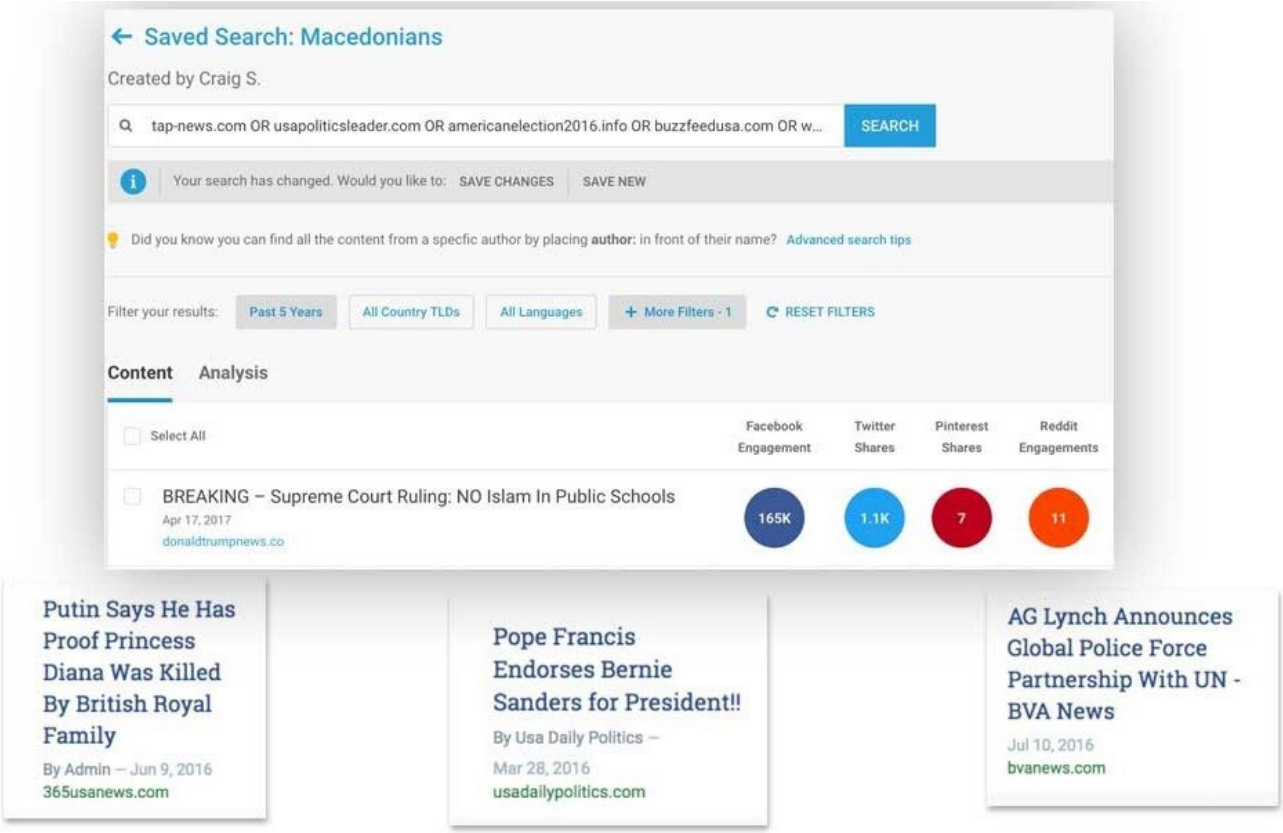
Një këshillë tjetër është të merrni URL-në e faqes dhe ta ngjisni në shiritat e kërkimit në Twitter. com ose Facebook.com. Kjo do t'ju tregojë nëse njerëzit po bëjnë lidhje me faqen. Gjatë një hetimi, hasa në një faqe, dentondaily.com. Faqja e saj kryesore tregonte vetëm disa artikuj nga fillimi i vitit 2020, por kur kërkova domenin në Twitter, pashë që më parë kishte nxjerrë shumë përmbajtje plagjiaturë, gjë që kishte bërë që njerëzit të vinin re këtë dhe të ankoheshin. Këto storie më të vjetra u fshinë nga faqja, por tuitet jepnin dëshmi për sjelljen e saj të mëparshme.



Pasi të keni gërmuar në përmbajtjen e një uebfaqeje, është koha për të kuptuar se si përhapet. Do të shohim dy mjete për këtë: BuzzSumo dhe CrowdTangle.

Në vitin 2016, punova me studiuesin Lorens Aleksander (Lawrence Alexander) për hulumtuar faqet e lajmeve politike amerikane që drejtoheshin nga jashtë. Së shpejti ne zbuluam faqet që drejtoheshin nga Velesi, një qytet në Maqedoninë e Veriut. I përdorëm detajet e regjistrimit të domenit (më shumë për këtë më poshtë) për të identifikuar më shumë se 100 faqe politike të SHBA-ve të drejtuara nga ai qytet. Doja të kuptoj se sa e popullarizuar ishte përmbajtja e tyre dhe çfarë lloj storiesh po publikonin. Mora URL-të e disa faqeve që dukeshin si më aktivet dhe krijova një kërkim për to në BuzzSumo, një mjet që mund të tregojë një listë të përmbajtjeve së një uebfaqeje të renditura sipas angazhimit që kanë marrë në Facebook, Twitter, Pinterest dhe Reddit (ka një version falas, megjithëse produkti me pagesë ofron shumë më tepër rezultate).

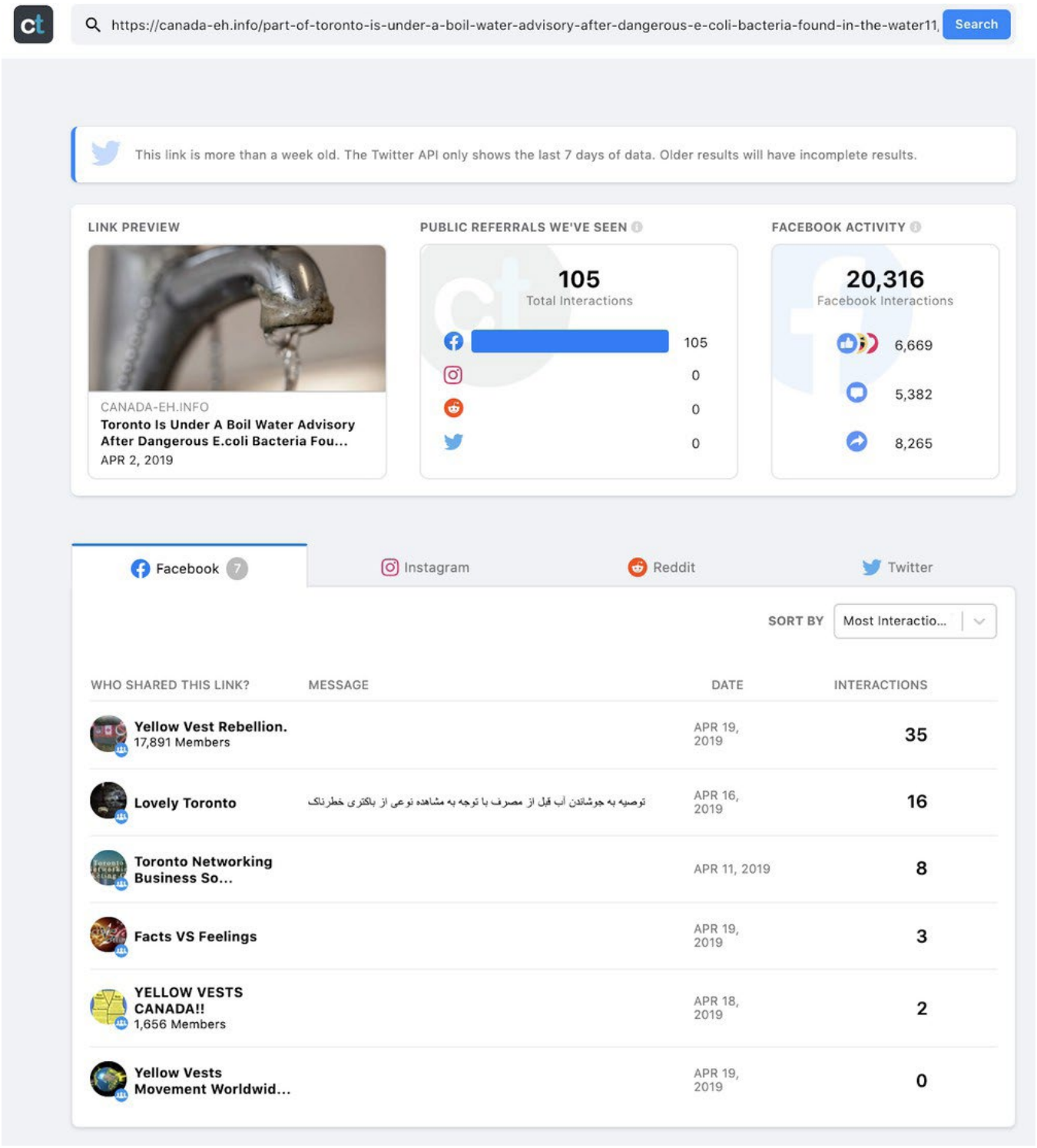
Menjëherë e pashë se artikujt nga këto faqe me më shumë angazhime në Facebook ishin krejtësisht false. Kjo na ofroi informacion kyç dhe një këndvështrim që ishte i ndryshëm nga raportimi i mëparshëm. Imazhi i mëposhtëm tregon ekranin të rezultateve të kërkimit të versionit bazik të BuzzSumo, i cili liston angazhimet e Facebook, Twitter, Pinterest dhe Reddit për një sajt specifik, si dhe disa shembuj të storieve të rreme nga viti 2016:



Një mënyrë tjetër për të identifikuar se si po përhapet përmbajtja e një uebfaqeje në Facebook, Twitter, Instagram dhe Reddit është të instaloni ekstensionin falas CrowdTangle për shfletuesit, ose të përdorni mjetin e tij në ueb për kërkim të linqeve. Të dyja ofrojnë të njëjtin funksionalitet, por le të punojmë me ueb versionin. (Këto mjete janë falas, por ju duhet një llogari në Facebook për pasur qasje).

Dallimi kryesor midis BuzzSumo dhe CrowdTangle është se ju mund të futni URL-në e një sajti në BuzzSumo dhe ai automatikisht do të shfaqë përmbajtjen më të angazhuar në atë faqe. CrowdTangle përdoret për të kontrolluar një URL specifike në një faqe. Pra, nëse futni buzzfeednews.com në CrowdTangle, do t'ju tregojë statistikat e angazhimit vetëm për atë faqe kryesore, ndërsa BuzzSumo do të skanojë të gjithë domenin për përmbajtjen e tij më të lexuar. Një tjetër ndryshim është se mjeti dhe ekstensioni për kërkim të linqeve i CrowdTangle do të shfaqin angazhimet në Twitter vetëm nga shtatë ditët e fundit. BuzzSumo ofron një numërim të shpërndarjeve të të gjitha kohërave në Twitter për artikujt në faqe.

Si shembull, futa URL-në e një storie të vjetër të rreme për një këshillë për ujë të vluar në Toronto në kërkimin e linqeve të CrowdTangle (faqja më vonë e fshiu storien, por URL-ja është ende aktive deri në shkrimin e këtij artikulli). CrowdTangle tregon se kjo URL ka marrë më shumë se 20.000 reagime, komente dhe shpërndarje në Facebook që nga publikimi i saj. Ai gjithashtu tregon disa nga faqet dhe grupet publike që shpërndanë linkun dhe ofron opsionin për të parë të dhëna të ngjashme për Instagram, Reddit dhe Twitter. Mbani mend: Tab-i për Twitter do të shfaqë tuitet vetëm nga shtatë ditët e fundit.



Vini re se numri i lartë i ndërveprimeve totale në Facebook nuk reflektohet realisht në listën e vogël të faqeve dhe grupeve që shohim. Kjo është, të paktën pjesërisht, për shkak se disa nga faqet kryesore që kanë përhapur linkun kur është publikuar për herë të parë janë hequr më vonë nga Facebook-u. Kjo është një përkujtim i dobishëm që CrowdTangle tregon të dhëna vetëm nga llogaritë aktive dhe nuk do t'ju tregojë çdo llogari publike që ka ndarë një URL të caktuar. Është një përzgjedhje, por është ende tepër e dobishme sepse shpesh zbulon një lidhje të qartë midis llogarive specifike të mediave sociale dhe një uebfaqeje. Nëse e njëjta faqe në Facebook shpërndan vazhdimisht - ose ekskluzivisht - përmbajtje nga një uebfaqe, kjo mund të sinjalizojë se ato drejtohen nga të njëjtët njerëz. Tani mund të gërmoni në faqe për të krahasuar informacionin me sajtin dhe për të identifikuar potencialisht personat e përfshirë dhe motivimet e tyre. Disa nga rezultatet e shpërndarjes së linqeve në Facebook të listuara në CrowdTangle mund të jenë gjithashtu të njerëzve që shpërndajnë artikullin në një grup në Facebook. Vini re llogarinë që ka ndarë linkun dhe shikoni nëse kanë shpërndarë përmbajtje të tjera nga faqja. Përsëri, pra, mund të ketë një lidhje.

Regjistrimi

Çdo emër domeni në ueb është pjesë e një data-baze qendrore që ruan informacionin bazë për krijimin dhe historinë e tij. Në disa raste, kemi fat të gjejmë edhe informacion për personin ose subjektin që ka paguar për të regjistruar një domen. Mund ta nxjerrim këtë informacion me një kërkim "whois", i cili ofrohet nga shumë mjete falas. Ekzistojnë gjithashtu një sërë mjetesh të shkëlqyera falas ose me çmim të ulët që mund të tregojnë informacion shtesë, si p.sh. kush ka zotëruar një domen me kalimin e kohës, serverët në të cilët është hostuar dhe detaje të tjera të dobishme.

Një paralajmërues është se është relativisht e lirë të paguash për të mbrojtur privatësinë e informacionit tuaj personal kur regjistroni një domen. Nëse bëni një kërkim "whois" në një domen dhe rezultati liston diçka si "Registration Private", "WhoisGuard Protected" ose "Perfect Privacy LLC" si regjistrant, kjo do të thotë se privatësia e domenit është e mbrojtur. Edhe në ato raste, prapëseprapë, një kërkim "whois" do të na tregojë datën kur domeni është regjistruar së fundmi, kur do të skadojë dhe adresën IP në internet ku është hostuar faqja.

DomainBigData është një nga mjetet më të mira falas për të hulumtuar një emër domeni dhe historinë e tij. Gjithashtu, në vend të një URL, mund të futni një e-mail ose një emër personi ose kompanie për të kërkuar sipas atyre të dhënave. Shërbime të tjera me kosto të përballueshme që mund të dëshironi t'i shënoni janë DNSlytics, Security Trails dhe Whoisology. Një opsion i shkëlqyeshëm, por më i shtrenjtë është produkti i hetimeve Iris nga DomainTools.

Për shembull, nëse fusim dentondaily.com në DomainBigData, mund të shohim se i është mbrojtur privatësia. Ai e liston emrin e regjistrantit si "Whoisguard Protected". Për fat të mirë, ne mund të shohim, prapëseprapë, se është regjistruar së fundmi në gusht të vitit 2019.

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	

Për një shembull tjetër, le të kërkojmë newsweek.com në DomainBigData. Menjëherë shohim se pronari nuk ka paguar për mbrojtjen e privatësisë. Aty është emri i një kompanie, një adresë e-maili, numra telefoni dhe faksi.

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	

Shohim gjithashtu se ky entitet e ka në pronësi domenin që nga maji i vitit 1994 dhe se faqja aktualisht është e hostuar në adresën IP 52.201.10.13. Gjëja tjetër që duhet të theksohet është se emri i kompanisë, e-maili dhe adresa IP janë secila të theksuar si linqe. Kjo do të thotë se ata mund të na çojnë në domene të tjera që i përkasin Newsweek LLC, domains@ibtimes.com dhe uebfaqeve të tjera të hostuara në të njëjtën adresë IP. Këto lidhje janë tepër të rëndësishme në një hetim, kështu që është gjithmonë e rëndësishme të shikoni domenet e tjera që janë pronë e personit ose subjektit të njëjtë.

Sa i përket IP adresave, kini kujdes se uebfaqet që nuk kanë fare lidhje mes tyre mund të hostohen në të njëjtin server. Kjo është zakonisht sepse njerëzit përdorin të njëjtën kompani për hostim për uebfaqet e tyre. Një rregull i përgjithshëm është që sa më pak uebfaqe hostohen në të njëjtin server, aq më shumë ka gjasa që të kenë lidhje mes tyre. Por kjo nuk është një gjë që mund të pohohet me siguri.

Nëse shihni qindra faqe të hostuara në një server, ato mund të mos kenë lidhje pronësie. Por nëse shihni se janë vetëm nëntë, për shembull, dhe ajo që ju intereson i ka informacion reg-

jistrimi me privatësi, ia vlen të bëni një kërkim “whois” në për tetë domenet e tjera për të parë nëse mund të kenë një pronar të përbashkët dhe nëse është e mundur që ai person zotëron gjithashtu faqen që po e hetoni. Njerëzit mund të paguajnë për mbrojtjen e privatësisë në disa ueb domene, por neglizhojnë ta bëjnë atë për të tjerat.

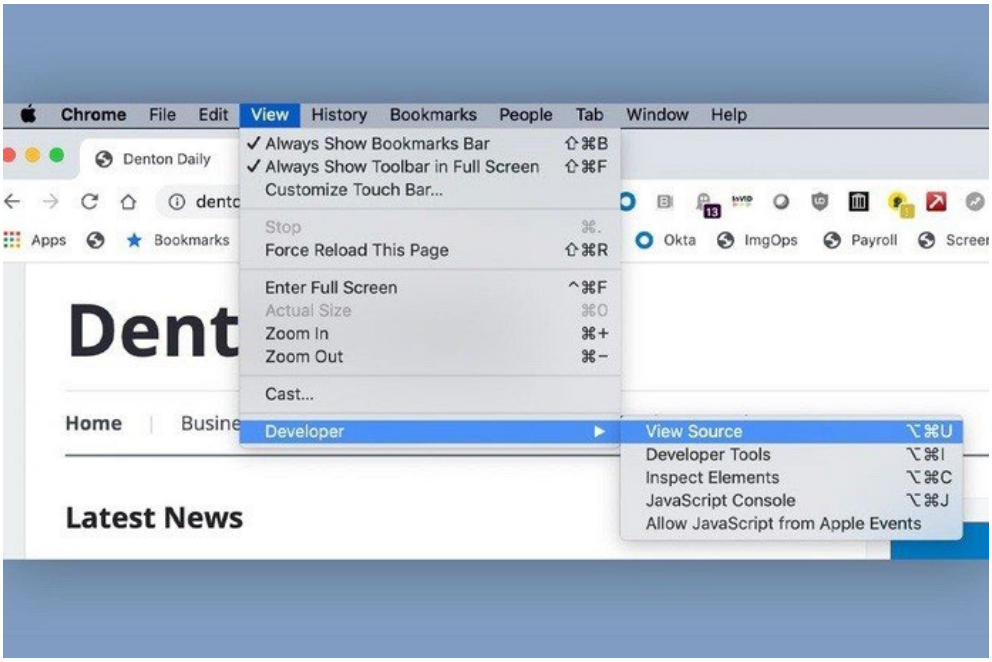
Lidhja e faqeve duke përdorur informacionin për IP, përmbajtjen dhe/ose regjistrimin është një mënyrë themelore për të identifikuar rrjetet dhe aktorët prapa tyre.

Tani le të shohim një mënyrë tjetër për të lidhur faqet duke përdorur kodin e një uebfaqeje.

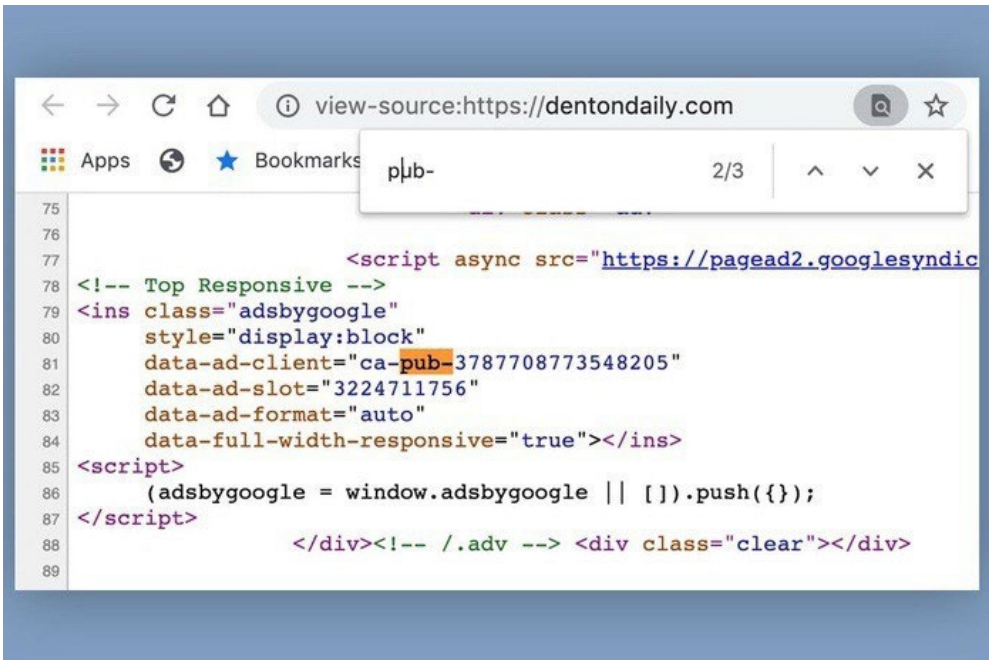
Kodi dhe analitika

Kjo qasje, e zbuluar fillimisht nga Lorens Aleksander, fillon me shikimin e kodit burimor të një uebfaqeje dhe më pas kërkimin brenda saj për të parë nëse mund të gjeni një kod Google Analytics dhe/ose Google AdSense. Këto janë produkte jashtëzakonisht të popullarizuara nga Google që, përkatësisht, i mundësojnë një pronari të faqes të gjurmojë statistikat e një uebfaqeje ose të fitojë para nga reklamat. Pasi të integrohet në një faqe, çdo uebfaqe do të ketë një ID unike të lidhur me llogarinë Analytics ose AdSense të pronarit. Nëse dikush drejton më shumë faqe, ata shpesh përdorin të njëjtën llogari Analytics ose AdSense për t’i menaxhuar ato. Kjo i jep një hulumtuesi mundësinë për të lidhur faqe në dukje të ndara duke gjetur të njëjtën ID në kodin burimor. Për fat të mirë, kjo është e lehtë për t’u bërë.

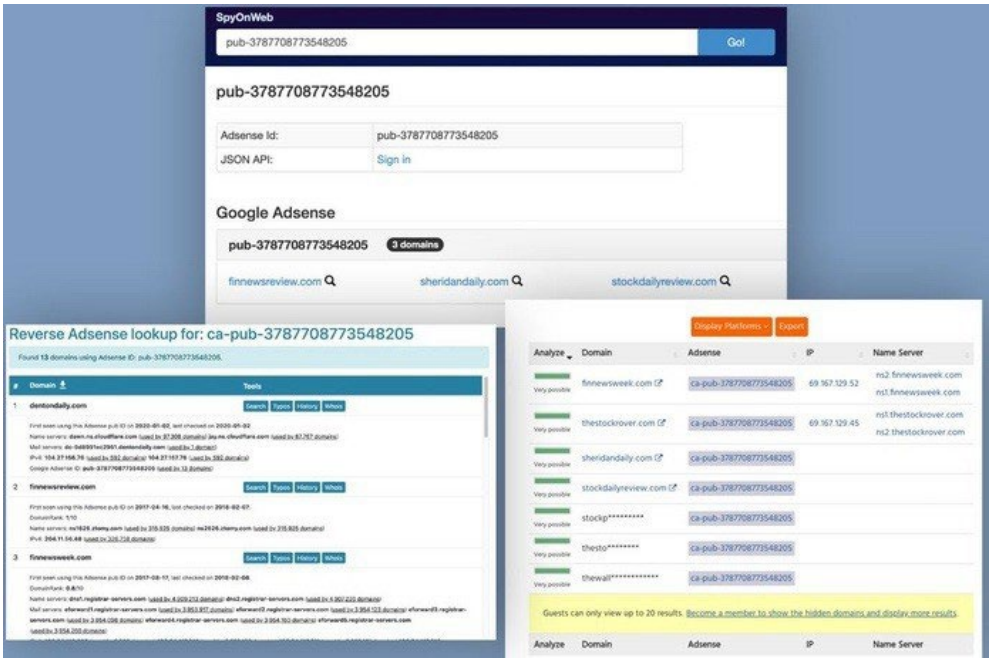
Së pari, shkoni në uebfaqen tuaj të synuar. Le të përdorim dentondaily.com. Në Chrome për Mac, zgjidhni menynë “Shiko” (View) më pas “Zhvillues” (Developer) dhe “Shiko burimin” (View Source). Kjo hap një skedë (tab) të re me kodin burimor të faqes. (Në Chrome për PC, shtypni ctrl-U.)



Të gjitha ID-të e Google Analytics fillojnë me “ua-” dhe më pas kanë një varg numrash. ID-të e AdSense kanë “pub-” dhe një varg numrash. Më pas mund ta gjeni në kodin burimor thjesht duke bërë një kërkim “find” në faqe. Në një Mac, shkruani command-F; në një kompjuter PC bëhet me ctrl-F. Kjo hap një kuti të vogël kërkimi. Futni “ua-” ose “pub-” dhe më pas do të shihni çdo ID brenda faqes.



Nëse e gjeni në ID, kopjoni dhe ngjiteni në kutinë e kërkimit në shërbime të tilla si SpyOnWeb, DNSlytics, NerdyData ose AnalyzeID. Vini re se shpesh merrni rezultate të ndryshme nga secili shërbim, prandaj është e rëndësishme të testoni një ID dhe të krahasoni rezultatet. Në imazhin e mëposhtëm, mund të shihni që SpyOnWeb gjeti tre domene me të njëjtën ID të AdSense, por DNSlytics dhe AnalyzeID gjetën disa të tjera.



Ndonjëherë një faqe ka pasur një ID në të kaluarën, por nuk është më e pranishme. Kjo është arsyeja pse është thelbësore të përdoret e njëjta “view source” qasje për çdo faqe tjetër që

supozohet se i ka të listuara këto ID për të konfirmuar se a janë të pranishme. Vini re se ID-të e AdSense dhe Analytics janë ende të pranishme në versionin e arkivuar të një faqeje në Wayback Machine. Pra, nëse nuk gjeni një ID në një faqen e drejtpërdrejtë, sigurohuni që të kontrolloni në Wayback Machine.

Të gjitha këto shërbime japin disa rezultate falas. Por shpesh është e nevojshme të paguani për të marrë rezultatet e plota, veçanërisht nëse ID-ja juaj është e pranishme në një numër të madh faqesh të tjera.

Një shënim përfundimtar për inspektimin e kodit burimor: ia vlen të skanoni faqen e plotë edhe nëse nuk kuptoni HTML, JavaScript, PHP ose gjuhë të tjera të zakonshme programimi në ueb. Për shembull, njerëzit ndonjëherë harrojnë të ndryshojnë titullin e një faqeje ose uebfaqeje nëse ripërdorin të njëjtin model/mostër (template) dizajni. Ky gabim i thjeshtë mund të ofrojë një pikë lidhjeje.

Ndërsa hetoja skemën e mashtrimit të reklamave me kompanitë parësore si Atoses, isha i interesuar për një kompani të quajtur FLY Apps. Shikova kodin burimor të uebfaqes së saj njëfaqëshe dhe afër fillimit të kodit të sajtit pashë fjalën "Loocrum" në tekst të thjeshtë (theksimi i shtuar):

```
317 <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/1G6hf/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; "/>
318 <span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
    </div>
319 <span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
    </form>
320 <span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box; "></span>
    </div>
321 <span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box;
    display:table;clear:both;"> </span></div>
322 <span style="box-sizing: border-box; -moz-box-sizing: border-box; -ms-box-sizing: border-box;
    display:table;clear:both;"> </span></div>
323 <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>
324 <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>
325 <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>
326 <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>
```

Kërkimi i kësaj fjale në Google nxori një kompani të quajtur Loocrum që përdorte të njëjtin dizajn të faqes në internet si FLY Apps dhe kishte të disa përmbajtje të njëjta. Një kërkim "Whois" zbuloi se adresa e e-mailit e përdorur për regjistrimin e loocrum.com ishte përdorur gjithashtu për të regjistruar kompani të tjera guaskë që i kisha identifikuar më parë në skemë. Kjo lidhje midis FLY Apps dhe Loocrum siguroi dëshmi të rëndësishme shtesë se katër burrat që drejtonin FLY Apps ishin të lidhur me këtë skemë të përgjithshme. Dhe kjo u zbulua thjesht duke lëvizur (bërë scroll) nëpër kodin burimor duke kërkuar fjalë me tekst të thjeshtë që dukeshin të vendosura pavend.

Përfundim

Edhe me të gjitha qasjet dhe mjetet e mësipërme në dispozicion, ndonjëherë mund të ndjeheni sikur keni hyrë në një qorr-sokak. Por shpesh ka një mënyrë tjetër për të gjetur lidhje ose rrugë për hulumtime të mëtejshme në një uebfaqe. Klikoni çdo link, studioni përmbajtjen, lexoni kodin burimor, shikoni se kujt i është kredituar faqja, shikoni se kush po e shpërndan atë, dhe shqyrtoni çdo gjë tjetër për të cilën mendoni se mund të zbulojë se çfarë po ndodh në të vërtetë.

9. Analizimi i reklamave në rrjetet sociale

Shkruan: Johana Uajlld

Johana Uajlld *(Johanna Wild) është një hulumtuese e burimeve të hapura në Bellingcat, ku fokusohet në teknologji dhe zhvillimin e mjeteve për hulumtime digjitale. Ajo ka përvojë në fushën e gazetarisë onlajn, e më parë ka punuar me gazetarë në rajone (post)konflikti. Një nga rolet e saj ishte t'i përkrahë gazetarët në Afrikën Lindore për të prodhuar transmetime për Zërin e Amerikës.*

Reklamat që shihni në kronologjinë (timeline) e mediave tuaja sociale nuk janë të njëjtat që i shohin në kronologjitë e tyre njerëzit që ulen pranë jush në transportin publik. Bazuar në faktorë të tillë si lokacioni juaj, gjinia, mosha dhe gjërat që i keni pëlqyer ose keni shpërndarë në rrjet, mund t'ju shfaqen reklama për suita luksoze për pushime në Malaga, ndërsa fqinji juaj shikon reklama për lojërat japoneze për telefona celularë.

Mikro-targetimi, kategorizimi i përdoruesve në grupe të synuara për t'u treguar atyre reklama që u përshtaten rrethanave dhe interesave të tyre të jetës, është bërë një shqetësim i madh gjatë zgjedhjeve. Shqetësimi është se fushatat mund të synojnë pjesë shumë të vogla të popullsisë me reklama që nxisin frikë ose urrejtje, ose që përhapin informacion të rremë. Në përgjithësi, reklamat e politikanëv re të vendosura në rrjetet sociale nuk i nënshtrohen verifikimit të fakteve. Facebook-u, për shembull, në janar të vitit 2020 riafirmoi se do të vazhdojë të lejojë çdo reklamë politike për sa kohë që i përmbahet standardeve të komunitetit të Facebook-ut. Kjo do të thotë se grupe të veçanta përdoruesish mund të synohen me reklama që përmbajnë dezinformata mbi tema vendimtare politike ose shoqërore.

Deri kohët e fundit, ishte pothuajse e pamundur për gazetarët dhe studiuesit të merrnin njohuri mbi reklamat që synonin (targetonin) përdorues të ndryshëm. Në përgjigje të kritikave publike për mungesën e transparencës, disa rrjete sociale krijuan biblioteka reklamash që lejojnë këdo të shqyrtojë informacionin rreth reklamave të publikuara në platformat e tyre.

Në veçanti, biblioteka e Facebook-ut është akuzuar se nuk i shfaq në mënyrë të besueshme të gjitha reklamat e disponueshme. Pra, sa herë që përdorni këto biblioteka, merrni pak kohë për të kontrolluar nëse të gjitha reklamat që shihni në kronologjinë tuaj mund të gjenden gjithashtu atje.

Bibliotekat e reklamave janë megjithatë një hap i rëndësishëm drejt transparencës më të madhe dhe u ofrojnë gazetarëve dhe të tjerëve mënyra të reja të mahnitshme për të hetuar reklamat digjitale. Teknikat e mëposhtme do t'ju ndihmojnë të filloni hetimin e reklamave të vendosura në platformat kryesore si Google, Twitter dhe Facebook.

Google (Gugëll)

Qendra e reklamave e Google është e fshehur mirë brenda Raportit të transparencës të tij. Përdorni këtë link për të hyrë në seksionin e reklamave politike, i cili ofron informacion mbi reklamat e Google dhe YouTube që vijnë nga Bashkimi Evropian, India dhe Shtetet e Bashkuara të Amerikës.

Faqja për çdo rajon tregon një listë të vendeve dhe shpenzimet totale të reklamave që nga fillimi i bërjes së raportit.

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 ›

Klikoni mbi një shtet dhe do kjo t'ju dërgojë në një faqe që përmban bazën e të dhënave të reklamave:

View ads

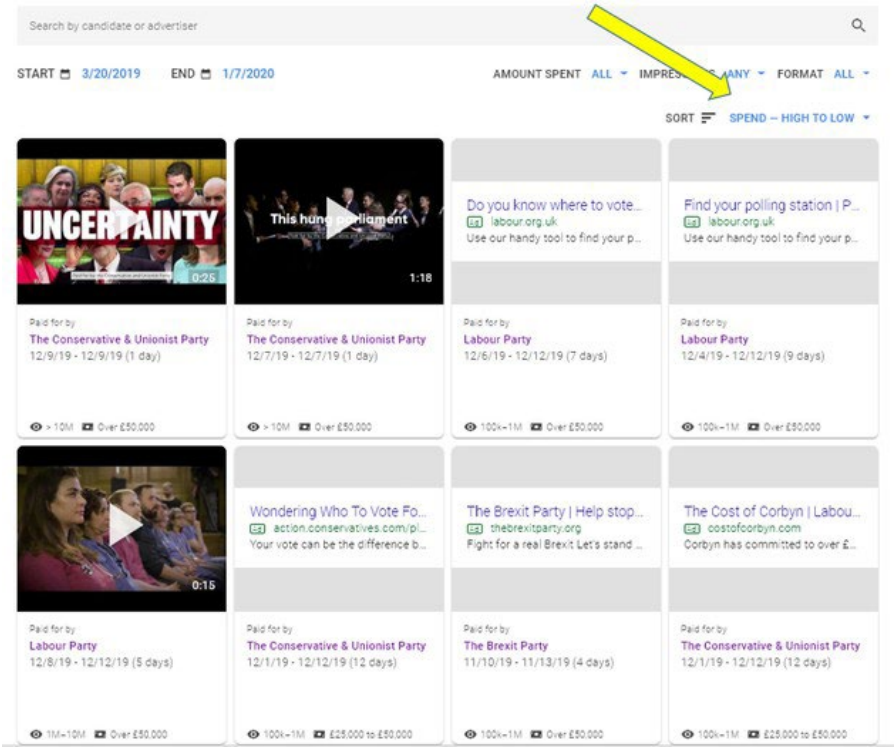
Search by candidate or advertiser

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

SORT MOST RECENT

Mund të filtroni rezultate sipas datës, sasisë së parave të shpenzuara dhe numrit se sa herë një reklamë u është shfaqur përdoruesve (përshtypjet - impressions). Mund të filtroni sipas formatit të reklamës nëse dëshironi të shikoni rezultatet për reklama me video, imazhe ose ato të bazuara në tekst.

Është gjithashtu e lehtë të gjesh shpenzuesit më të mëdhenj. Për shembull, nëse doni t'i shihni fushatat më të mëdha të reklamave politike të vendosura në Mbretërinë e Bashkuar që nga fillimi i raportit deri në janar të vitit 2020, thjesht ndryshoni kategorinë "rendit"(sort) në "shpenzim - i lartë në të ulët" (spend - high to low), siç tregohet më poshtë.

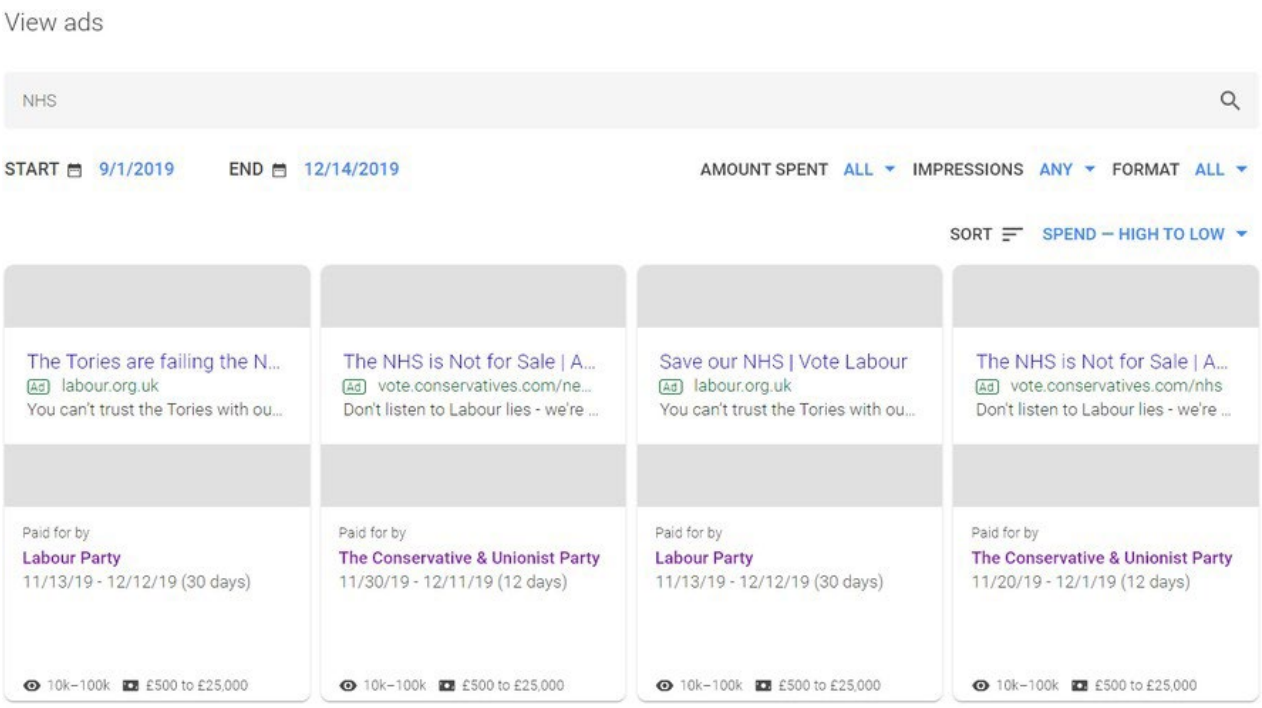


Nuk është për çudi që blerjet më të mëdha të reklamave erdhën pak para dhe në ditën e Zgjedhjeve të përgjithshme, më 12 dhjetor 2019. Mund të shihni gjithashtu se Partia Konservatore dhe Unioniste investoi më shumë se £50,000 për secilën prej dy reklamave në YouTube që u shfaqën vetëm për një ditë.

Partia Laburiste, për krahasim, shpenzoi më shumë se £50,000 për një reklamë në faqet e rezultateve të kërkimit të Google për një mjet që tha se mund të ndihmonte votuesit të gjenin qendrën e tyre të votimit.

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.

Gjithashtu, mund të kërkoni me fjalë kyçe. Shkruani NHS (për Shërbimin Shëndetësor Kombëtar) dhe do të shihni se në nëntor dhe dhjetor të vitit 2019 Partia e Laburiste dhe Konservatorët blenë reklama kërkimi në Google për të kritikuar planet e njëri-tjetrit për NHS.



Duke klikuar mbi emrin e reklamuesit, mund të kontrolloni gjithashtu shumën totale të parave që ata kanë shpenzuar në reklamat e Google që nga fillimi i Raportit të Transparencës. Ja se si dukej kjo për dy partitë kryesore politike në Mbretërinë e Bashkuar që nga janari 2020:

Gjithashtu mund të shikoni një kronologji të shpenzimeve të tyre. Raportet në të majtë trego-jnë paternin (shabllonin) e shpenzimeve për Partinë Konservatore dhe Unioniste, e ai në të djathtë është për Partinë Laburiste:

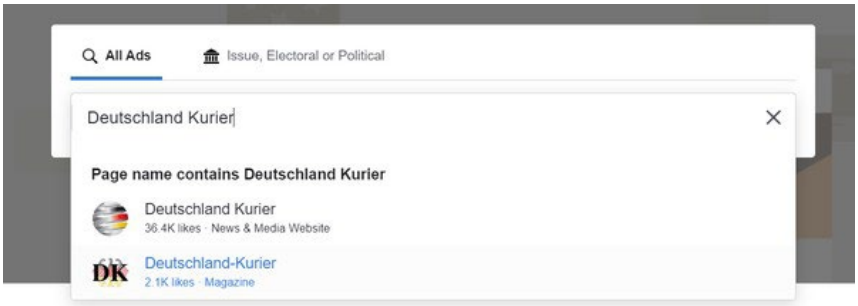
Nëse dëshironi të analizoni më tej bazën e të dhënave të reklamave, lëvizni (scroll) poshtë de-risa të shihni një seksion të gjelbër të quajtur "shkarkoni të dhënat" (download data), i cili ju lejon të shkarkoni të dhënat në formatin CSV.

Kjo ju mundëson të importoni të dhënat në një program fletëllogaritës (spreadsheet) si Google Sheets ose Excel, në mënyrë që të mund të kryeni filtrim dhe analizë shtesë.

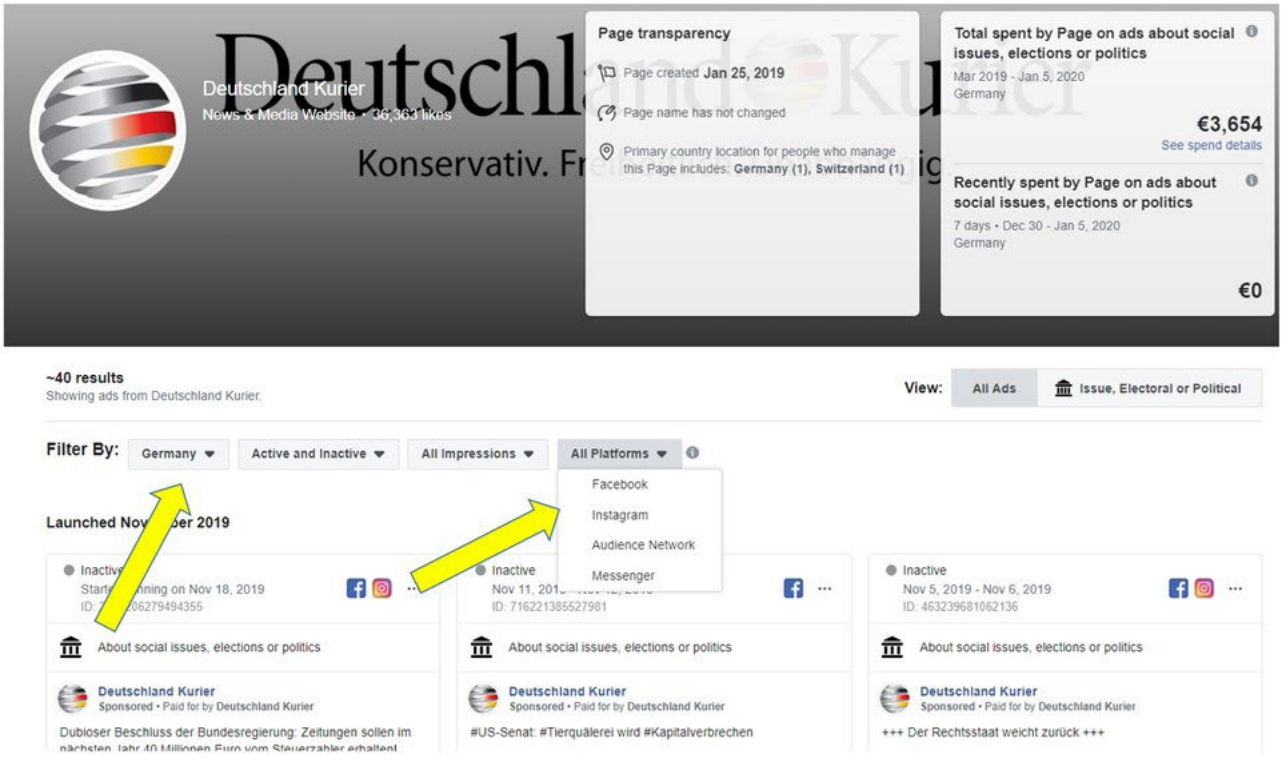
Facebook (Facebook)

Biblioteka e reklamave në Facebook është e ndarë në dy pjesë: "Të gjitha reklamat" (All Ads) dhe "Çështje, zgjedhore ose politike" (Issue, Electoral or Political). Nëse klikoni në "Të gjitha reklamat", mund të kërkoni për reklamues të veçantë vetëm me emër, në vend që të përdorni gjithashtu fjalë kyçe.

Për shembull, nëse dua të shoh reklama nga Deutschland Kurier, një botim që shpesh publikon përmbajtje në mbështetje të partisë gjermane të ekstremit të djathtë AFD, mund të shkruaj emrin e tij dhe Facebook-u do të rekomandojë faqe me atë tekst:

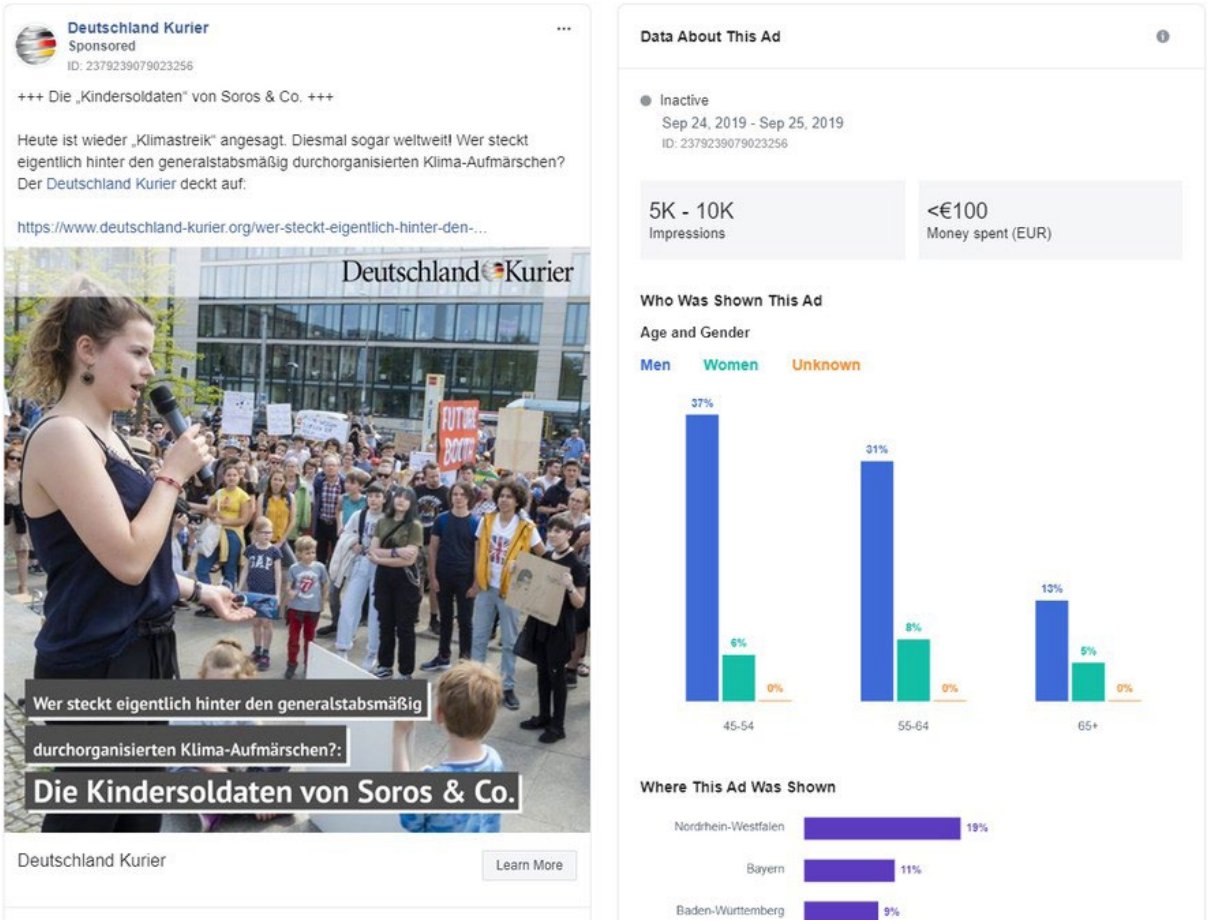


Faqja e rezultateve tregon se Deutschiand Kurier ka vendosur reklama me vlerë 3.654 euro në Gjermani midis marsit 2019 dhe janarit të vitit 2020.



Pasi të jeni në faqen e rezultateve, sigurohuni që të zgjidhni shtetin e duhur për kërkimin tuaj (ose "të gjitha" - all) dhe të zgjidhni nëse dëshironi të shihni reklama nga Facebook, Instagram, Messenger ose nga Facebook Audience Network (Rrjeti i audiencës në Facebook). Rrjeti i audiencës është një rrjet reklamash i operuar nga Facebook-u që vendos reklama në aplikacionet celulare dhe uebfaqet të ndryshme nga ato në pronësi të Facebook-ut. Në shumicën e rasteve, zgjidhja më e mirë do të jetë kërkimi në të gjitha platformat për të marrë një pamje të plotë të reklamave të një organizate.

Në një reklamë individuale mund të klikoni butonin "Shiko detajet e reklamës" (See ad details) për të parë informacion shtesë.



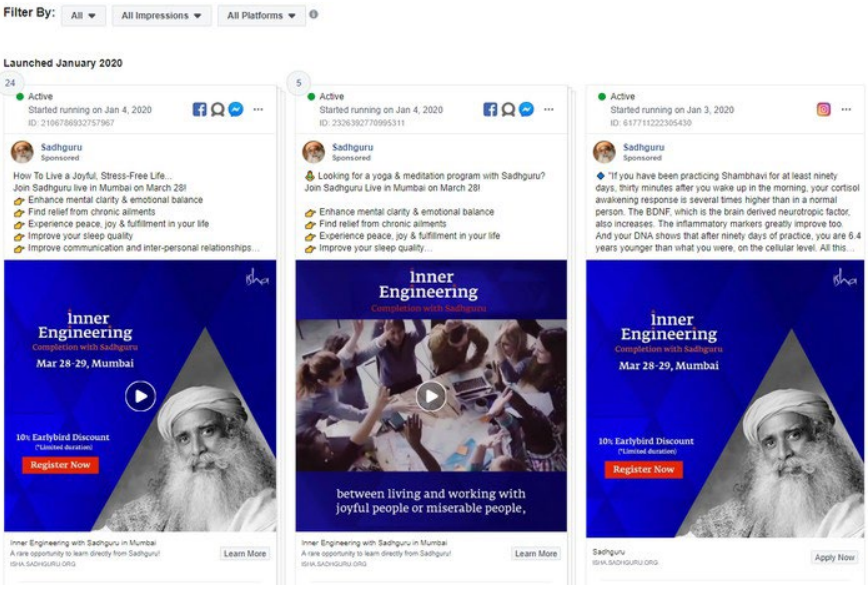
Në këtë rast, Deutschland Kurier shpenzoi më pak se 100 euro për këtë reklamë që i quan protestuesit e ndryshimeve klimatike "fëmijë ushtarë të Soros & Co." dhe kishte midis 5.000 dhe 10.000 përshtypje, kryesisht të shfaqura për burrat e moshës 45 vjeç e lart.

Opsioni i dytë për të kërkuar bibliotekën e reklamave është të zgjidhni bazën e të dhënave "Çështje, zgjedhore ose politike", e cila është një arkiv reklamash për "çështje shoqërore, zgjedhje ose politikë". Përparësia e madhe i këtij opsioni është se mund të kërkoni për çdo fjalë kyçe që ju pëlqen, dhe këto lloj reklamash arkivohen nga Facebook-u.

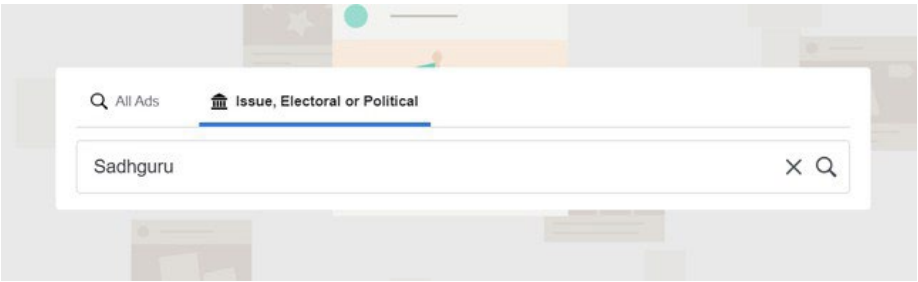
Të shohim një shembull.

Sadhguru është emri i një figure të njohur shpirtërore indiane, që thotë se nuk është i lidhur me asnjë parti politike. Ai ka thënë se e sheh si detyrë të tij të mbështesë çdo qeveri aktuale "që të bëjnë më të mirën që munden". Nëse shkruani emrin e tij në seksionin "Të gjitha reklamat"(All Ads), Facebook-u sugjeron faqen personale të Sadhguru në Facebook.

Kjo na tregon një përzgjedhje të reklamave apolitike të publikuara nga Sadhguru ku ai promovon kurset e tij të jogës dhe meditimit.



Tani, le të shkruajmë emrin e tij në shiritin e kërkimit "Çështje, zgjedhore ose politike" pa pranuar sugjerimet e faqes që dalin në Facebook:



Rezultatet ndryshojnë në mënyrë drastike. Tani mund të shihni një koleksion reklamash që përmendin emrin e Sadhguru të publikuar nga llogari të tjera.

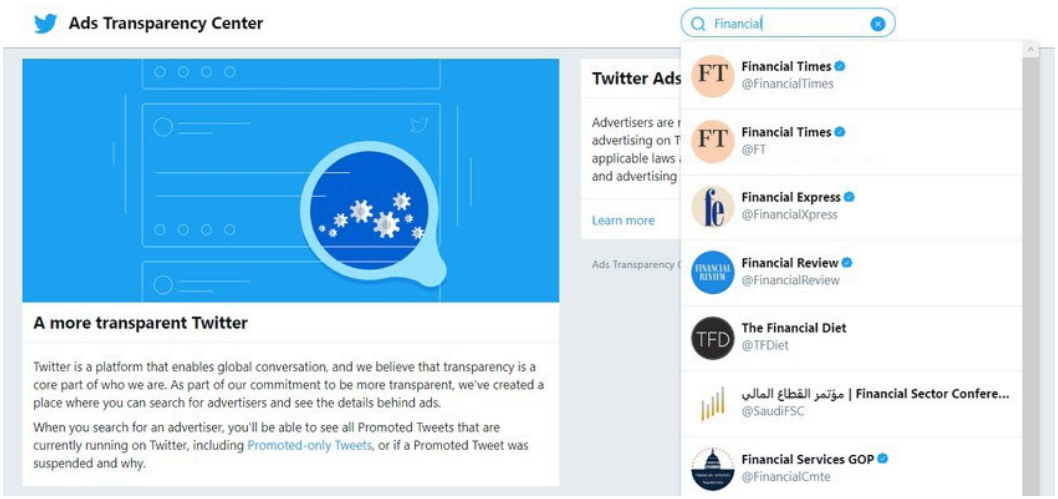
Një reklamë nga partia nacionaliste indiane BJP në pushtet tregon një video në të cilën Sadhguru shpreh mbështetjen e tij për projekt-ligjin e diskutueshëm të partisë për Amendamentin e Shtetësisë. Projektligji i lejon emigrantët e paregjistruar nga disa prej vendeve fqinje të Indisë që të fitojnë më lehtë shtetësinë indiane, por nuk u jep të njëjtën mundësi myslimanëve. Reklama ofron një indikacion për marrëdhënien e mundshme midis Sadhguru dhe BJP, një temë që diskutohet gjerësisht në Indi.

Ky shembull tregon se si të përdorni bibliotekën e reklamave të Facebook-ut për të shtuar informacione kyçe në hulumtimet tuaja. Gjithashtu, mund t'i hidhni një sy raportit të bibliotekës së reklamave në Facebook, i cili i nxjerr informacionet kryesore nga reklamat politike në shtete të ndryshme.

Twitter (Twitter)

Në fund të vitit 2019, Twitter-i vendosi të ndalojë reklamat politike në platformën e tij. Megjithatë, është ende e mundur të përdoret qendra e transparencës së reklamave të rrjetit social për të marrë informacion rreth reklamave jopolitike në shtatë ditët e fundit.

Gjetja e reklamave është e rëndë sepse nuk ka funksionalitet të kërkimit të fjalëve kyçe. Për të filluar një kërkim, shkoni te kutia në këndin e sipërm djathtas dhe shkruani një emër përdoruesi ose dorezë (handle) specifike.



Nëse ka pasur reklama në shtatë ditët e fundit, tani do t'i shihni ato të listuara.

Duke kërkuar për "The Financial Times", mund ta shohim se ka paguar reklamë në përpjekje për të gjeneruar më shumë interes për storien e tij "Si munden folësit vendas të mos i nga të gjithë të tjerët" ("How native speakers can stop confusing everyone else"). Tuiti është dërguar më 3 dhjetor 2019, por informacioni i reklamës nga Twitter nuk detajon se kur u filloi të rrjedhë saktësisht ky promovim me pagesë.

Për të shpejtuar kërkimet tuaja, mund të përdorni një truk të vogël. Pasi të keni kryer një kërkim, hidhini një sy URL-së në shfletuesin tuaj:

URL-ja përdor gjithmonë të njëjtën strukturë, me një dorezë Twitter në fund. Thjesht fshini pjesën e fundit dhe zëvendësojeni me një dorezë tjetër:

ads.twitter.com/transparency/FinancialTimes

URL-ja përdor gjithmonë të njëjtën strukturë, me një dorezë Twitter në fund. Thjesht fshini pjesën e fundit dhe zëvendësojeni me një dorezë tjetër:

ads.twitter.com/transparency/Bellingcat

Rifreskoni faqen dhe tani do të shihni informacionin e reklamave për Bellingcat. Nëse ajo llogari nuk ka lëshuar asnjë reklamë në shtatë ditët e fundit, do të shihni mesazhin "Kjo llogari nuk ka promovuar asnjë reklamë në shtatë ditët e fundit". Meqenëse mund të shihni vetëm reklama nga shtatë ditët e mëparshme, gjëja më e mirë që mund të bëni është të kontrolloni shpesh për të parë nëse një llogari që keni shënuar ka shfaqur reklama dhe të bëni skrinshote sa herë që shihni reklama të reja.

Snapchat (Snepçet)

"Biblioteka e reklamave politike Snap" (Snap political ads library) ofron vështrim mbi reklamat politike, "të lidhura me çështje" (issue related), ose reklama të avokimit. Këto të fundit përkufizohen si "reklama që kanë të bëjnë me çështje ose organizata që janë temë debati në nivel lokal, kombëtar ose global, ose janë me rëndësi publike". Për shembull, tema të tilla si emigracioni, arsimi ose armët.

Nëse hyni në bibliotekë, do të shihni një listë të viteve.

Archives

2018

2019

2020

Klikoni në një nga vitet dhe mund të shkarkoni një tabelë me të gjitha informacionet e disponueshme rreth reklamave të atij viti. Përmbajtja e tabelës nuk duket shumë mahnitëse në pamje të parë, por në fakt është! Çdo rresht përfaqëson një reklamë dhe ju tregon se kush e ka vendosur reklamën, sasinë e parave të shpenzuara për të, madje edhe cilat karakteristika janë zgjedhur për të mikro-targetuar përdoruesit.

16 3e4c8332c 2,64E+08 l
17 a5b7f6d8c362e1810d41be049569f0a76fb80a6020411bfa5e5f0a4744df484c,https://www.snap.com/political-
18 ads/asset/a0ee86600cda141a006c4a4c60c5d4dd9c78f23dbf08a3ac9329b51fa5d76fe6?mediaType=mp4,EUR,315,417284,2020/01/06 05:30:55Z,2020/01/11 22:30:55Z,Ja zum Schutz,CH,Ja zum Schutz,Ja
19 zum Schutz,,18+,switzerland,,"Fribourg,Geneve,Jura,Neuchatel,Ticino,Valais,Vaud",,,,,,,,,"Adventure Seekers,Arts & Culture Mavens,Beachgoers & Surfers,Beauty Mavens,Bookworms & Avid
20 Readers,Collegiates,Foodies,Hipsters & Trendsetters,Political News Watchers,Outdoor & Nature Enthusiasts,Pet & Animal Lovers,Philanthropists,Worldly Travelers,Women's Lifestyle",,Provided by
21 Advertiser,"de,en",,,,web_view_url:https://jazumschutz.ch/fahne-snap
22 cfb4d1da728d946f5fbcec8b9e409f76150ba9e1a6764228e42eb76082b7b5f8,https://www.snap.com/political-ads/asset/6fcf8e70b0690c182e8b3fcad40f512578f75c1df3708fe59f248505520a3ef3?mediaT

Në shembullin e mësipërm, reklamuesi ka dashur të targetojë "Kërkuesit e aventurës, mjeshtrit e arteve dhe kulturës. Adhuruesit e plazheve dhe surferët, kampionët e bukurisë, adhuruesit a librave dhe lexuesit e pasionuar, studentët, të pasionuarit pas ushqimit, hipsterët dhe nxitësit e trendeve, shikuesit e lajmeve politike, entuziastët e natyrës dhe peizazheve, dashamirët e kaf-shëve, filantropët, udhëtarët e botës, ata që duan stilin e jetës së grave."

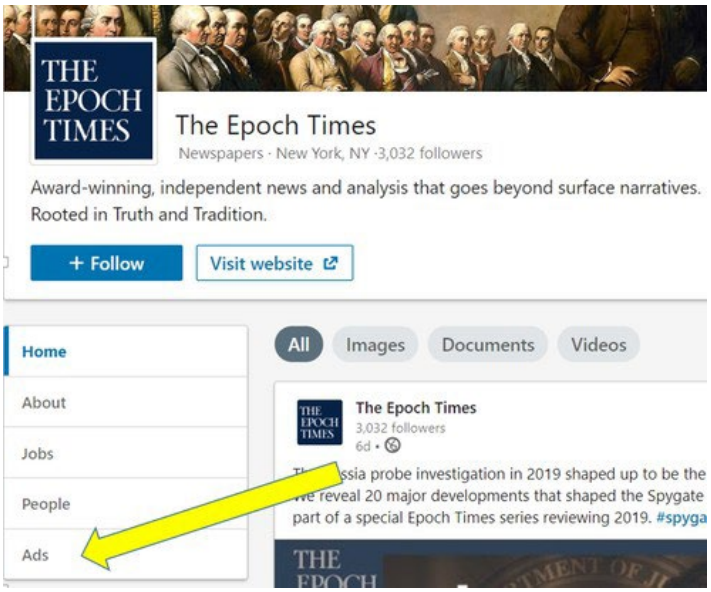
Platformat e tjera nuk ofrojnë këtë lloj informacioni të targetimit në bibliotekat e tyre të reklamave.

Gjithashtu, në tabelë do të gjeni një URL që ju lejon të shihni reklamën aktuale. Në këtë shembull, gjeta një mesazh që i inkurajonte njerëzit të porosisin falas flamuj me ylber në mbështetje të një votimi të ardhshëm në Zvicër lidhur me mbrojtjen kundër diskriminimit të personave LGBT.

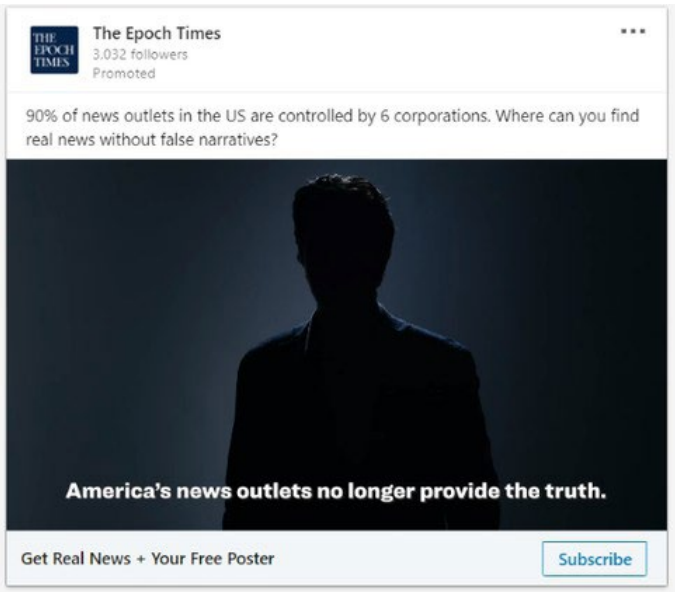
LinkedIn (Linkdin)

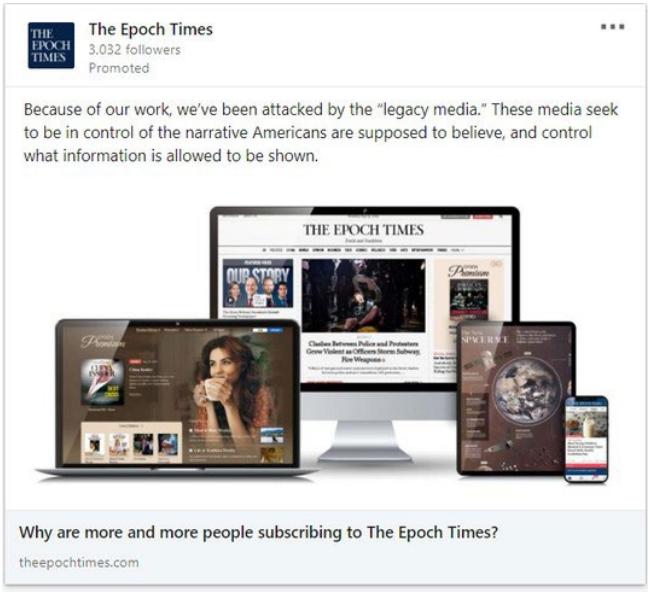
LinkedIn nuk lejon reklama politike në platformën e tij dhe nuk ka një bibliotekë reklamash. Për fat të mirë, ka një mënyrë tjetër për të marrë informacion për reklamimin një kompanie specifike në platformë.

Nëse shkoni në faqen e kompanisë LinkedIn, do të shihni një skedë të quajtur "Reklamat"(Ads) në fund të kolonës së majtë.

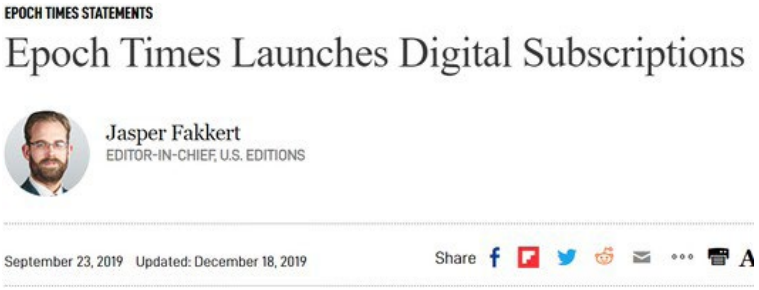


Klikoni në atë skedë dhe LinkedIn do t'ju tregojë një listë të të gjitha reklamave të publikuara nga kjo kompani në gjashtë muajt e mëparshëm. Duke përdorur këtë mjet, ishte e mundur të shihej se Epoch Times po publikonte ende reklama në LinkedIn pasi ishte ndaluar të bënte të njëjtën gjë në Facebook. Dy reklamat e kompanisë pretendonin se "mediat e lajmeve të Amerikës nuk japin më të vërtetën" dhe bënin kontrast me këtë pretendim duke paraqitur The Epoch Times si "media të pavarur" dhe "jopartiake".





Datat e sakta të publikimit nuk janë të dukshme, por mund të klikoni në reklamë (kjo do të funksionojë edhe nëse nuk është aktive në LinkedIn) dhe, ndonjëherë, faqja e destinacionit ofron një datë më konkrete. Reklama e parë e Epoch Times çoi në një tekst të datës si "23 shtator 2019" dhe "I përditësuar: 18 dhjetor 2019", që ndihmoi në vlerësimin se kur mund të ishte onlajn.



Pasi të njiheni me mundësitë e tyre të fshehura, bibliotekat e reklamave janë një mjet shtesë i lehtë dhe i fuqishme për arsenalin tuaj për hulumtim digjital dhe një element i rëndësishëm për të kontrolluar kur hetoni një person ose entitet me prani në media sociale.

10. Gjurmimi i aktorëve nëpër platforma

Shkruan: Ben Kolins

Ben Kolins *(Ben Collins) është reporter i NBC News që mbulon dezinformatat, ekstremizmin dhe internetin. Për pesë vitet e fundit, ai ka raportuar për rritjen e teorive konspirative, komunitetet e urrejtjes, fushatat e manipulimit të huaj dhe dështimet e platformave. Ai ka punuar më parë në The Daily Beast, ku ekipi i tij zbuloi llogaritë, grupet dhe ngjarjet e jetës reale të krijuara nga ferma e trollëve të Agjencisë Ruse të Kërkimeve në Internet gjatë zgjedhjeve të vitit 2016 në SHBA.*

Më 3 gusht 2019, Patrik Krusius (Patrick Crusius) hyri në një Walmart në El Paso dhe vrau 22 njerëz në një incident të armatosur me motive të nacionalizmit të bardhë. Por, përpara se të hynte në shitore, ai postoi një manifest në bordin/sondazhin e diskutimit politik në 8chan.net, një tabelë mesazhesh anonime, e cila në vitet e fundit është kthyer në një vend grumbullimi për nacionalistët e bardhë. Bordet e diskutimit politik në 4chan dhe 8chan janë pothuajse tërësisht të pamoderuara, dhe deri në verën e vitit 2019, 8chan ishte bërë një vend grumbullimi i përmbajtjes dhe diskutimit nacionalist të bardhë e të dhunshëm.

Pjesërisht për shkak të kësaj, përdoruesit e 8chan ndonjëherë paralajmëronin autoritetet dhe gazetarët kur postohej një manifest i ri dhe i dhunshëm. Kjo bëhej duke shtuar komente poshtë vetë manifestit dhe përmes paraqitjeve dhe lajmërimeve onlajn te mediat ose te organet e zbatimit të ligjit. Kur sulmuesi në El Paso paraqiti për herë të parë manifestin e tij – i cili fillimisht u shfaq me një shtojcë të gabuar – një përdorues u përgjigj "Përshëndetje FBI". Manifesti i saktë u postua më pas drejtpërdrejtë nën komentin që jepte sinjalin për FBI-në.

Ky lloj vetë-raportimi mund të jetë informacion kritik për gazetarët në vigjilje të këtyre tragjedive. Në disa raste, përdoruesit me paksa vullnet të mirë do të shkojnë në pjesë më të hapura dhe më të popullarizuara, civile të uebit si Reddit dhe Twitter për të raportuar manifeste ose postime të dyshimta të bëra përpara të shtënave. Kjo është thelbësore, sepse është e lehtë të huqësh një postim ose koment relevant në 4chan dhe 8chan.

Platformat anonime si 4chan dhe 8chan luajnë një rol të rëndësishëm në ekosistemin e informatave të gabuara (misinformata) dhe dezinformatave onlajn, sepse ato janë aty ku njerëzit shpesh punojnë së bashku për të krijuar dhe koordinuar fushatat. Reddit, një tjetër vend i njohur ku përdoruesit janë kryesisht anonimë, është nikoqir (hoston) një grup të larmishëm të onlajn komuniteteve. Disa janë subreddit-e që moderohen shumë e që mund t'i ndihmojnë përdoruesit të shkëmbejnë storie rreth hobive ose të diskutojnë lajme dhe ngjarje; të tjerët janë në thelb të lirë për çdo gjë (free-for-alls) ku urrejtja mund të zhvillohet pa ndalur. Është thelbësore që gazetarët të dinë se si të monitorojnë dhe raportojnë për të gjitha këto komunitete, dhe të dinë kompleksitetin e mënyrës se si funksionojnë ato.

Duke pasur parasysh këtë, këtu janë pesë rregulla që duhen respektuar kur ngjarjet kërkojnë që të përdorni 4chan ose 8chan (ose replikimin e tyre më të ri, 8kun) për informacionin e raportimit tuaj:

1. Mos besoni asgjë në 4chan/8chan.
2. Mos besoni asgjë në 4chan/8chan.
3. Mos besoni asgjë në 4chan/8chan.
4. Disa informacione të dobishme që kanë të bëjnë me (ose edhe prova për) një krim, fushate të trollimeve ose dezinformata mund të gjenden në 4chan/8chan.
5. Mos besoni asgjë në 4chan/8chan.

Nuk mund të theksoj se sa e rëndësishme është që reporterët të ndjekin rregullat 1, 2, 3 dhe 5, edhe nëse kjo i pengon për të marrë disa nga "lëngjet" e rëndësishme që mund të mblidhen nga numri 4. Këto uebfaqe janë të zhvilluara që të trollojnë, të përhapin aludime dhe të pavërteta për armiqtë e perceptuar, të shtyjnë gënjeshtra për njerëzit e margjinalizuar dhe, herë pas here, të postojnë gënjeshtra kuazi-qesharake të përshtatura si storie të vërteta për atë se si është të jesh adoleshent.

Kjo dëshmohet nga fakti se ato janë përdorur si deponi (plehrash) për manifeste të nacionalistëve të bardhë, incel-ëve (njerëz që konsiderojnë veten joatraktivë dhe që shfaqin urrejtje ndaj femrave dhe meshkujve atraktivë), dhe të meshkujve tjerë të dëshpëruar - gjuajtës me armë.

Ta themi edhe një herë: Nëse është në 4chan ose 8chan (që do të vazhdojmë t'i referohemi si 8chan nga këtu e tutje, pavarësisht ndryshimit të emrit të tij thjesht nominal në 8kun), ka gjasa shumë të mira që është një gënjeshtër që synon të mbjellë kaos dhe rrëmujë te reporterët. Mos hyni në një fill (thread) për të kërkuar më shumë detaje. Mos postoni asgjë, në fakt. Do të jeni në shënjestër të njerëzve që kanë shumë kohë në dispozicion.

Konfirmimi i manifestit

Kjo është arsyeja se pse është kaq e dobishme kur anëtarët e këtyre komuniteteve bëjnë përpjekje për të lajmëruar për manifeste ose përmbajtje të tjera të vlefshme për lajme. Komenti "Përshëndetje FBI" në 8chan është se si mësova për ekzistencën e manifestit të El Pasos. Menjëherë pas raportimeve për të shtënat, kërkova në Twitter me fjalët kyçe "El Paso 4chan" dhe "El Paso 8chan". Kërkimi për "[emri i qytetit] + [8chan ose 4chan ose incels.co] ose faqe të tjera ekstremiste ofron një shabllon të dobishëm për çdo ngjarje të ngjashme.

Kërkimi im në Twitter zbuloi se disa përdorues kishin ndarë skrinshotet e postimeve të gjuajtësit në 8chan, megjithëse shumica ia kishin atribuuar gabimisht postimin dikujt në 4chan. Kështu që më duhej të kërkoja postimin.

Cila është mënyra më e shpejtë për të kërkuar një postim 8chan? Google. Pas të shtënave, kërkova për "site:8ch.net" dhe më pas shtova një pjesë të një fjalie nga postimi i supozuar në 8chan nga sulmuesi. (Shënim: 4chan fshin automatikisht postimet nga serverët e tij pas një periudhe të caktuar kohore, por ka faqe automatike të arkivimit 4chan. Më e plota quhet 4plebs.org. Postimet e arkivuara në 4chan mund të gjenden thjesht duke zëvendësuar 4chan në URL me 4plebs, dhe duke hequr prefiksin "boards". Për shembull: boards.4chan.org/jDol/13561062.html mund të gjendet në at4plebs.org/jDol/13561062.html.)

Gjatë disa ndodhive me gjuajtje me armë zjarri, mund të jetë e dobishme të provoni të kërkoni për "site:4chan.net + 'manifesto' ose 'fbi'" dhe të përdorni opsionet e kërkimit të Google për të kufizuar kornizën tuaj kohore në 24 orët e fundit. Përdoruesit e Chan-it mund të kenë tentuar tashmë të denoncojnë sulmuesin në përgjigje të postimit të tyre.

Strategjia ime fillestare e kërkimit nuk shfaqi postimin përkatës të 8chan, gjë që më bëri të besoja se ky ishte një mashtrim i krijuar shpejt. Por diçka nuk ishte siç duhet. Postimi i paraqitur në skrinshotin në Twitter, në fakt, kishte një ID të përdoruesit dhe numrin e postimit. Këto detaje më bënë të mendoj se ishte i vërtetë, e jo një falsifikim i thjeshtë. Në 8chan, çdo postim vjen nga një ID unik i përdoruesit, i cili gjenerohet algoritmikisht dhe shfaqet pranë datës së postimit. Ky sistem u lejon përdoruesve të kenë një ID statike në mënyrë që të mund të identifikojnë veten brenda një thread-i (filli).

Ky sistem ID i përdoruesit, meqë ra fjala, është se si njerëzit e dinë se "Q" nga teoria e konspiracionit QAnon është në të vërtetë ai. Përdoruesit mund të krijojnë de fakto emra përdoruesish dhe fjalëkalime të përhershme duke futur një emër përdoruesi në fushën e ID-së kur bëjnë një postim, të pasuar me një #, e më pas edhe nga një fjalëkalim.

Kjo ID e përdoruesit është shkak se pse e dija që i njëjti person, i cili postoi gabimisht PDF-në me emrin e gjuajtësit në të, ishte i njëjti përdorues si ai që postoi manifestin aktual dy minuta më vonë. Të dy postimet e ndanin të njëjtin ID të përdoruesit të krijuar rastësisht: 58820b.

Pranë një ID të përdoruesit është një numër postimi, i cili është një artefakt disi i përhershëm që krijon një URL unike për çdo postim. Skrinshoti i manifestit të El Pasos të shpërndarë në Twitter përfshinte një ID të postimit "No.13561062". Kjo krijon URL-në 8ch.net/pol/res/13561062.html. Mund ta përdorni këtë konventë të URL-së si në 4chan ashtu edhe në 8chan.

Mirëpo, në këtë rast, postimi nuk ekzistonte. Mendova se ndoshta sepse ishte fshirë. (Më vonë mësova se pronari i 8chan Xhim Uotkins e kishte hequr atë pasi u lajmërua për përmbajtjen e tij.)

Meqë postimi ishte zhdukur, shpresa ime më e mirë ishte se ai ishte arkivuar nga dikush që e ka njohur rëndësinë e tij. Fatmirësisht, një përdorues i 8chan që mendon shpejt e ka ruajtur postimin në faqen e arkivit archive.is. Duke ngarkuar URL-në në kutinë "Dua të kërkoj arkivin për fotografi të ruajtura" " (I want to search the archive for saved snapshots) të archive.is, zbuloi se postimi i manifestit ishte i vërtetë dhe tani mund ta shikoja.

Por kishte një problem të ri: Kur është postuar për herë të parë në 8chan? Më duhej një vulë e saktë kohore (timestamp) për të konfirmuar se manifesti ishte postuar përpara se sulmuesi në El Paso të fillonte tërbimin e tij.

4chan dhe 8chan, të dyja lokalizojnë vulat e tyre kohore, duke e bërë një detyrë të ndërlikuar nxjerrjen e kohës reale nga faqet e arkivimit. Për fat të mirë, ka një mënyrë të pagabueshme për këtë. Duke klikuar me të djathtën mbi vulën kohore dhe duke klikuar "inspect element" do të shfaqet kodi burimor i sajtit dhe do të nënvizojë një seksion që fillon me '<time unixtime='[number]'."

Kopjojeni dhe ngarkojeni atë numër në një konvertues të vulave kohore Epoch/Unix, si unixtimestamp.com, dhe do të fitoni vulën kohore të dytë, në zonën kohore UTC. Konvertimi nga zona kohore UTC në zonën kohore të El Pasos zbuloi se manifesti u postua në orën 10:15 të mëngjesit me Kohë Qendrore – disa minuta para fillimit të të shtënave.

Kjo punë më ndihmoi të konfirmoja se manifesti i postuar në manifestin e 8chan ishte, në fakt, një provë legjitime në një rasti të terrorizmit racist të brendshëm.

Gjurmimi i aktorëve nëpër platforma

Në vitin 2017, Lejn Dejvis (Lane Davis), një ish "hulumtues i Gamergate" (lexo: përndjekës profesionist i internetit) për figurën e turpëruar alt-djathtiste Milo Jianopulos, vrau babanë e tij në shtëpinë e tij.

Dejvis kishte hyrë në një debat me prindërit e tij dhe një telefonatë në 911 zbuloi se ai po përhapte internet zhargonin ekstremist të të djathtës së skajshme pak para sulmit. Ai iu referua prindërve të tij si "pedofilë majtistë" përpara se babai i tij të thërriste policinë për ta ndihmuar që të dëbonte Dejvisin nga shtëpia e tyre, ku jetonte ende djali i tij.

Dejvis onlajn njihej si "Seattle4Truth", dhe në videot e YouTube ai shpesh u referohej rretheve fiktive sekrete të pedofilëve që ai besonte se ishin forca lëvizëse që qëndron prapa liberalizmit. Një video në YouTube me emrin e tij titullohej, "Lidhjet e thella të ideologjisë progresive me pedofilinë".

Skenari i ëndrrave për një gazetar në hetimet e ekstremizmit në internet është një autor i krimit që përdor emër përdoruesi statik nëpër platforma, dhe ky ishte rasti me Dejvisin. Ai e identifikoi veten si Seattle4Truth në YouTube dhe në Reddit, ku postimet e tij zbuluan një tru që ishte edhe më i mbushur me konspiracion.

Si u zbulua kjo? Duke vendosur thjesht seattle4truth në konventën e URL-së së emrit të përdoruesit të Reddit: reddit.com/u/[username]. Pasi të jeni atje, mund t'i kategorizoni sipas postimeve më të reja, postimeve më të popullarizuara dhe më "kontroverse", gjë që i rendit postimet sipas kombinimit të numrit të herëve që janë votuar "për" ose "kundër".

Një mënyrë për të kërkuar shpejt një emër përdoruesi është përdorimi i Namechk, i cili kërkon një emër përdoruesi në afro 100 shërbime të internetit. Siç e detajoj më poshtë, kjo nuk do të thotë se këto llogari i drejton i njëjti person, por është një mënyrë efikase për të parë se ku përdoret emri i përdoruesit, në mënyrë që të mund të gërmoni dhe të hulumtoni. Gjithashtu, mund të kërkoni përmes Google çdo emër përdoruesi që ju intereson.

Është gjithashtu e rëndësishme të jeni të vetëdijshëm për llojin e komuniteteve super-niche të internetit, ku mund të jetë aktiv objektivi juaj. Një sulmues i vitit 2017 i një shkolle në Nju Meksiko, Uilliam Eduard Etçison (William Edward Atchison), u identifikua nga përdoruesit në KiwiFarms, një faqe e dedikuar kryesisht për bullizmin anti-trans, si @satanicdruggie. Përdoruesit thanë se ai ishte aktiv në Encyclopedia Dramatica, një faqe për meme të çfarëdo lloji, e cila ndonjëherë mund të hostojë retorikë ekstremiste.

Jo vetëm që Etçison ishte aktiv në Encyclopedia Dramatica, ai ishte një SysOp atje, që do të thotë se ai ishte një administrator dhe përdorues i fuqishëm. (Ne konfirmuam me përdoruesit e sajtit që zhvilluan marrëdhënie reale, të përqendruara në Skype me Etçison se llogaritë ishin të tijat. Etçison do t'i drejtonte vullnetarisht përdoruesit në llogari të tjera të tijat, në rast të ndonjë ndalese.) Një kërkim në Google i emrit të tij të përdoruesit duke përdorur vargun "site:encyclopediadramatica.rs + [username]" zbuloi se ai ka përdorur emrin Satanic Druggie, por edhe emra si "Future School Shooter" (Gjuajtës shkolle i ri) dhe "Adam Lanza", emri i gjuajtësit në Sendi Huk (Sandy Hook).

Historia e postimeve të tij nëpër ueb zbuloi një obsesion me të shtënat në shkollë që as policia nuk e zbuloi vigjiljen e të shtënave.

Është përsëri e rëndësishme të theksohet se prania e një emri përdoruesi nëpër platforma nuk garanton që llogaritë janë krijuar nga një person. Në një shembull të famshëm, agjentët famëkeq të dezinformimit të së djathtës ekstreme, Ian Majlls Çeong (Ian Miles Cheong), Majk Cernoviç (Mike Cernovich), InfoWars dhe GatewayPundit, të gjithë pretenduan se një njeri që vrau dy persona dhe plagosi 10 të tjerë në një turne video lojërash në Xheksonvill ishte kundër Trampit.

Arsyeja e tyre? Sulmuesi, Dejvid Kac (David Katz), përdorte emrin e përdoruesit "Ravens-2012Champs" në turnetë e video lojërave në internet, e një përdorues anti-Tramp në Reddit kishte një emër përdoruesi të ngjashëm: "RavenChamps".

Raportimi ishte sa pa frymë, aq edhe i pasaktë. Titulli i InfoWars thoshte: "Gjuajtësi i çmendur i Xheksonvill kritikoi 'Tramptard-ët' në Reddit", kurse storia pretendonte se ai "i urrente mbështetësit e Trampit".

Siç u tregua, RavenChamps ishte një person krejtësisht tjetër, një punëtor i fabrikës në Minesotë me emrin Pavel.

"Unë jam gjallë e dini?" shkroi ai në Reddit disa orë pas të shtënave. (Gjuajtësi i vërtetë vrau veten pasi kreu masakrën.)

Ju nevojitet shumë më tepër sesa thjesht një emër përdoruesi, por ai mund të jetë një pikënisje kyçe për të çuar më tej raportimin tuaj, ndërsa kontaktoni organet e ligjit, gërmoni në të dhënat publike dhe bëni telefonata.

Gjurmimi i fushatave afërsisht me kohën reale

Fushatat e dezinformimit dhe manipulimit mediatik shpesh përhapen në Reddit dhe 4chan, dhe disa janë të gjurmueshme në kohë reale.

Për shembull, 4chan ka qenë në biznesin e manipulimit të onlajn sondazheve për të rritur kandidatët e preferuar për vite me radhë. Në vitin 2016, postuesit e 4chan postuan në mënyrë të përsëritur linqe me faqet e lajmeve kombëtare dhe hiper-lokale që organizonin sondazhe në vigjiljen e debateve që shfaqnin kandidatin e preferuar të bazës së përdoruesve, Donald Tramp.

Ndryshimi i parametrave të kërkimit në Google për të filtruar sipas postimeve në "orën e fundit", e më pas kërkimi "site:4chan.org 'polls'" do t'ju japë një pasqyre mjaft të mirë për sondazhet që përdoruesit e 4chan po përpiqen të manipulojnë në kohë reale.

Kjo ka vazhduar edhe në ciklin e ardhshëm zgjedhor. Sondazhet e 4chan e avanconin Tulsi Gabbard, të cilin ata e quanin "Mami", në sondazhet në The Drudge Report dhe NJ.com. Duke përdorur atë kërkim të thjeshtë në Google, çdokush mund të shihte rezultatet e sondazhit të zhvendosura në kohë reale pasi një përdorues i Chan-it u tha përdoruesve "JEPJANI ASAJ FUQINË TUAJ".

Është edhe më e lehtë të shikohen operacione aktive të trollimit në sajte si /The_Donald community i Reddit-it për shkak të mjetit të dobishëm të "ngritjes" (rising) që e ka Reddit.

Përdorimi i konventës "reddit.com/r/[subreddit-name]/rising" tregon rezultate që po fitojnë fuqi në një shpejtësi të pazakontë në një subreddit në çdo orë të caktuar.

Gjithashtu mund të shikoni postimet që janë me mbi-performancë në të gjithë platformën duke përdorur: reddit.eom/r/all/rising. Kjo indekson çdo postim në shumicën e komuniteteve të Reddit. Nuk bën kërkim në subreddit-e të karantinuara, të cilat janë komunitete toksike me një shprehi për përmbajtje thellësisht fyese dhe që synojnë komunitetet e tjera me fushata trollimi. Subreddit-ët e karantinuar gjithashtu nuk indeksohen në Google, por "reddit.com/r/[subreddit-name]/rising" do të funksionojë për ta. Karantinimi funksionon mirë për kufizimin e shtrirjes së fushatave me trollime jashtë audiencave të centralizuara, por e bën më të vështirë gjurmimin se si aktorët e këqij po organizohen në një moment.

Në përgjithësi, është një ide e mirë të ruani seksionin "në rritje" (rising) të komuniteteve të njohura për fushatat e trollimit, si r/the_donald, gjatë ngjarjeve të mëdha të lajmeve politike, tragjedive dhe zgjedhjeve.

Realiteti është se ndonjëherë gjërat që bëjnë këto platforma për të penguar aktorët e këqij mund ta bëjnë më të vështirë për gazetarët të bëjnë punë të rëndësishme. Mjetet mund të ndihmojnë, por shumë nga kjo është punë manuale dhe kërkon qasje për verifikim që nuk mund t'i riprodhojnë algoritmet dhe kompjuterët.

Në fund të fundit, një kompjuter nuk mund ta zëvendësojë këtë lloj pune. Ajo varet nga ne.

11. Analizimi dhe atribuimi i rrjeteve

Shkruan: Ben Nimo

Ben Nimo *(Ben Nimmo) është drejtor i hulumtimeve në Graphika dhe një bashkëpunëtor i lartë jorezident në Laboratorin e Kërkimeve Forenzike Digjitale të Këshillit Atlantik (Atlantic Council). Ai është i specializuar në studimin e informacionit ndër-platformë në shkallë të gjerë dhe të operacioneve të ndikimit. Kohën e lirë e kalon në zhytje nën ujë, ku nuk mund të kontaktohet me telefon.*

Kur kemi të bëjmë me ndonjë operacion të dyshuar informacioni, pyetja kyçe për një studiues është se sa i madh është operacioni dhe sa larg përhapet. Kjo është e ndarë nga matja e ndikimit të një operacioni, e cila është gjithashtu e rëndësishme: Gjithçka ka të bëjë me gjetjen e llogarive dhe faqeve të drejtuara nga vetë operacioni.

Për një hulumtues, qëllimi është të gjejë sa më shumë që të jetë e mundur nga operacioni përpara se të raportojë për të, sepse pasi të raportohet për operacionin, është e pritshme që operatorët mund të fshihen - potencialisht duke fshirë ose duke braktisur asete tjera.

Lidhja e parë në zinxhir

Në çdo hulumtim, gjurma e parë është më e vështira për t'u gjetur. Shpesh, një hetim do të fillojë me një denoncim nga një përdorues i shqetësuar ose (më rrallë) nga një platformë e mediave sociale. Puna e Laboratorit të Kërkimeve të Forenzikës Digjitale për të ekspozuar operacionin e dyshuar të zbulimit rus "Infektimi sekondar" (Secondary Infektion) filloi me një informatë nga Facebooku, i cili kishte gjetur 21 llogari të dyshuara në platformën e tij. Puna arriti kulmin gjashtë muaj më vonë, kur Graphika, Reuters dhe Reddit ekspozuan përpjekjen e të njëjtit operacion për të ndërhyrë në zgjedhjet britanike. Një hetim mbi dezinformatat që synonin (targetonin) veteranët amerikanë filloi me zbulimin nga një punonjës i Veteranëve të Vietnamit të Amerikës se grupi i tij po imitohej nga një faqe në Facebook me dy herë më shumë ndjekës sesa prania e tyre reale në platformë.

Nuk ka asnjë rregull të vetëm për identifikimin e lidhjes së parë në zinxhir përmes burimeve tuaja. Strategjia më efektive është të kërkoni të papërputhshmen. Mund të jetë një llogari Twitter me bazë në Tenesi, por e regjistruar në një numër telefoni celular rus; mund të jetë një faqe në Facebook që pretendon se është e vendosur në Nigjer, por menaxhohet nga Senegali dhe Portugalia. Mund të jetë një llogari në YouTube me një milion shikime që poston sasi të mëdha të përmbajtjes pro-kineze në vitin 2019, por pothuajse të gjitha shikimet e saj kanë qenë nga episodet e sitcom-eve britanike që janë ngarkuar në vitin 2016.

Mund të jetë një uebfaqe anonime që fokusohet në politikën e jashtme amerikane, por është e regjistruar në Departamentin e Financave të qarkut ushtarak të Lindjes së largët të Federatës Ruse. Mund të jetë një intervistë e supozuar me një "agjent të MI6" të shtruar në gjuhë anglishte të përsosur, pothuajse shekspiriane. Mund të jetë edhe një llogari Twitteri që ndërthur ftesat për një faqe pornografie me citate jo të plota nga "Ndjenjë dhe ndjeshmëri" e Xhejn Ostin (Jane Austen, "Sense and Sensibility").

Truku me të gjitha sinjalet e tilla është të gjesh kohë për të menduar për to. Hulumtuesit dhe gazetarët janë aq shpesh nën presion të kohës saqë është e lehtë të hidhen poshtë sinjalet duke menduar "kjo është vetëm e çuditshme" dhe duke vazhduar më tej. Shpesh, nëse diçka është e çuditshme, është e çuditshme për një arsye. Marrja e kohës për të thënë "Kjo është e çuditshme: Pse është kështu?" mund të jetë hapi i parë në ekspozimin e një operacioni të ri.

Asetet, sjellja, përmbajtja

Pasi të identifikohet aseti fillestar, si një llogari ose uebfaqe, sfida është të zbuloni se ku shpie ajo. Tre pyetje janë vendimtare këtu, të modeluara sipas "ABC-së të Dezinformimit" nga Kamill Fransoa (Disinformation ABC, Camille Francois):

- Çfarë informacioni për asetin fillestar është i disponueshëm?
- Çfarë sjellje kishte aseti?
- Çfarë përmbajtje ka postuar?

Hapi i parë është të grumbulloni sa më shumë informacion që të jetë e mundur për asetin fillestar. A është një uebfaqe, kur është regjistruar dhe nga kush? A ka ndonjë veçori të identifikueshme, të tilla si një kod i Google Analytics ose një numër AdSense, një adresë e-maili regjistrimi ose një numër telefoni? Këto pyetje mund të kontrollohen duke iu referuar të dhënave historike të Whois, të ofruara nga shërbime të tilla si lookup.icann.com, domaintools.com, domainbigdata.com ose faqja me emrin shqetësues 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

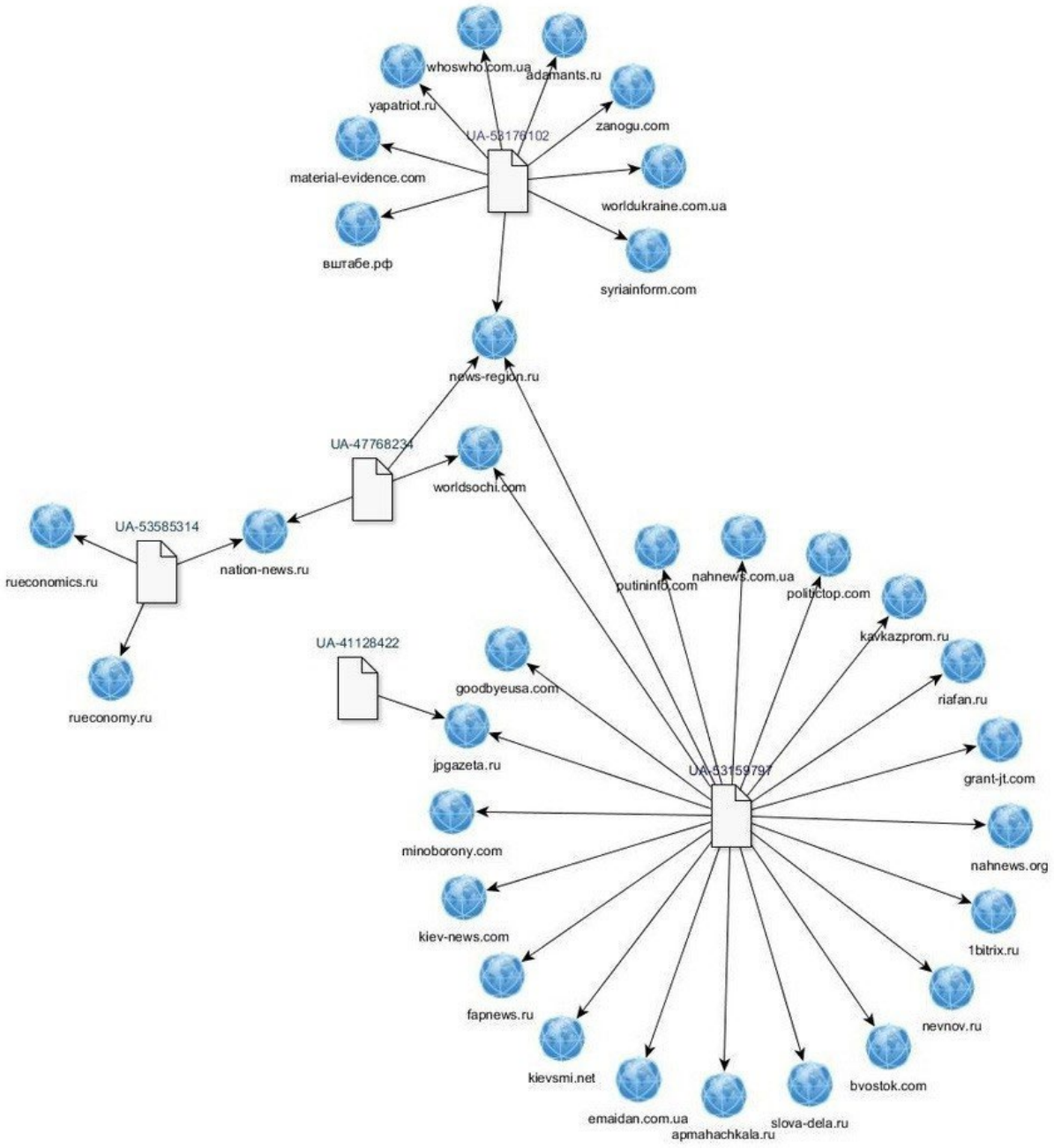
Registrant:

Name: Finance Department of the Far Eastern Military district

Detajet e regjistrimit në ueb për uebfaqen NBeneGroup.com, e cila pretendonte të ishte një "Grup i analizës së të rinjve", duke treguar regjistrimin e tij në Departamentin e Financave të qarkut ushtarak të Lindjes së largët të Federatës Ruse, nga lookup.icann.org.

Informacioni i uebfaqes mund të përdoret për të kërkuar më shumë asete. Uebfaqet domaintools.com dhe spyonweb.com, që ty dyja i lejojnë përdoruesit të kërkojnë sipas treguesve të tillë si adresa IP dhe kodi i Google Analytics, duke çuar potencialisht në uebfaqet të lidhura - megjithëse operacionet më të mira të informacionit tani zakonisht fshehin regjistrimin e tyre prapa subjekteve tregtare ose shërbimeve të privatësisë, duke e bërë këtë më të vështirë.

Një pjesë e hershme e analizës nga hulumtuesi britanik Lorens Aleksander (Lawrence Alexander) identifikoi 19 uebfaqe të drejtuara nga Agjencia Ruse e kërkimeve të internetit duke ndjekur numrat e tyre të Google Analytics. Në gusht të vitit 2018, firma e sigurisë FireEye ekspozoi një operacion ndikimi iranian në shkallë të gjerë, duke përdorur informacionin e regjistrimit, përfshirë e-mailet, për të lidhur uebfaqet që në dukje ishin të palidhura.



Rrjeti i uebfaqeve të lidhura përmes kodeve të tyre të Google Analytics (numra tetëshifrorë të prefiksuar me shkronjat UA), të identifikuar nga studiuesi britanik Lorens Aleksander

Nëse aseti fillestar është një llogari e mediave sociale, zbatohen udhëzimet e ofruara në dy kapitujt e mëparshëm në lidhje me botët dhe aktivitetin joautentik dhe hetimin e llogarive sociale. Kur u krijua? A përputhet emri i tij në ekran me emrin e dhënë në dorezën e tij? (Nëse doreza është "@moniquegrieze" kurse emri i ekranit është "Simmons Abigayle", është e mundur që llogaria të jetë e rrëmbyer ose pjesë e një përpjekjeje për krijimin masiv të llogarive).

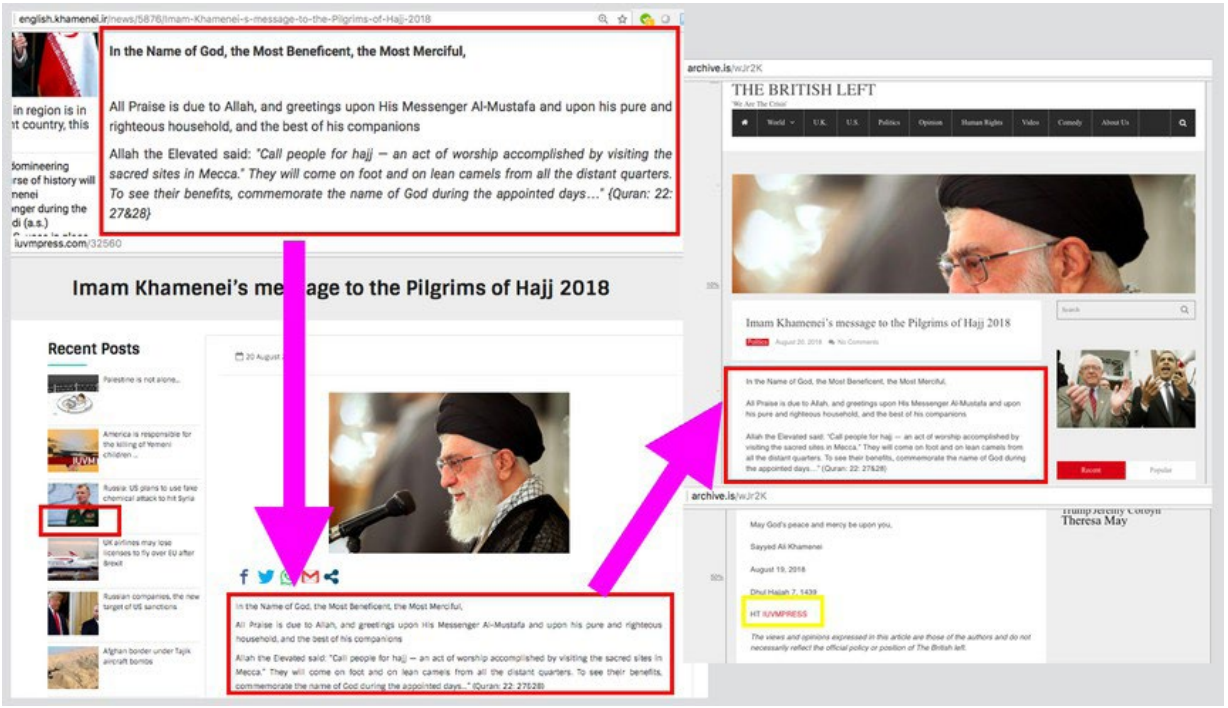
Tre llogari në Twitter të përfshira në një operacion të madh botësh në gusht 2017. Krahasoni emrat e ekranit me dorezat, që jep indicie se, me shumë mundësi, këto ishin llogari që ishin rrëmbyer, riemërtuar dhe ripërdorur nga "bariu i botëve".

A ofron ndonjë detaj biografik të verifikueshëm, apo lidhje me asete të tjera platformën e njëjtë apo platforma të tjera? Nëse është një faqe ose grup në Facebook, kush i menaxhon, dhe ku ndodhen? Kë e ndjek dhe kush e ndjek? Cilësimet e "Transparencës së faqes" dhe "anëtarëve të grupit" të Facebookut shpesh mund të japin të dhëna të vlefshme, siç mund të jenë veçoritë e profilit në Twitter, si data e anëtarësimit dhe numri i përgjithshëm i tuiteve dhe pëlqimeve. (Në Facebook dhe Instagram, nuk është e mundur të shihet data e krijimit të llogarisë, por data e ngarkimit të parë të fotografisë së profilit ofron një tregues të përafërt të arsyeshëm.)

Transparenca e uebfaqes dhe faqes në Facebook për sajtin e gjoja të kontrollit të fakteve "C'est faux — Les fake news du Mali" (Është e rreme - lajme të rreme nga Mali), që tregon se ajo pretendonte se drejtohej nga një grup studentësh në Mali, por në fakt drejtohej nga Portugalia dhe Senegali. Imazhi nga DFRLab.

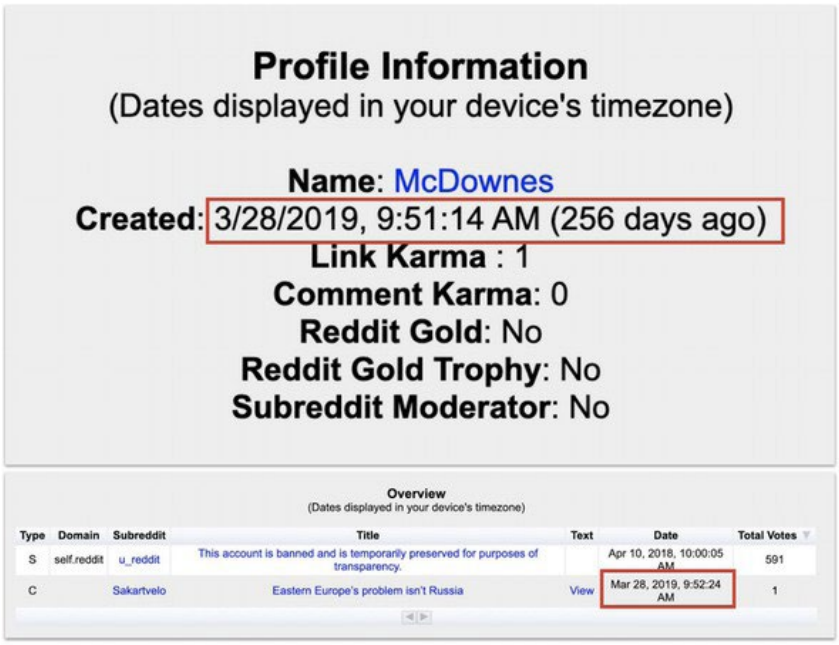
Pasi të jenë regjistruar detajet e asetit, hapi tjetër është karakterizimi i sjelljes së tij. Pyetja për test këtu është, "Cilat tipare të sjelljes janë më tipike për këtë aseti dhe a mund të jenë të dobishme për të identifikuar asete të tjera në të njëjtin operacion?"

Kjo është një pyetje e gjerë dhe mund të ketë shumë përgjigje, disa prej të cilave mund të dalin vetëm në fazat e mëvonshme të një hetimi. Mund të përfshijë, për shembull, YouTube kanale që kanë emra dhe fotografi të profilit perëndimore, por postojnë video politike në gjuhën kineze të ndërthurura me sasi të mëdha videosh të shkurtra TikTok. Mund të përfshijë rrjete të llogarive në Facebook ose Twitter që ndajnë gjithmonë lidhje me të njëjtën uebfaqe, ose të njëjtin koleksion uebfaqesh. Mund të përfshijë llogari që përdorin të njëjtin formulim, ose variacione të afërta të të njëjtit formulim, në biografinë e tyre. Mund të përfshijë persona "gazetarë" që nuk kanë detaje biografike të verifikueshme, ose që japin detaje që mund të identifikohen si të rreme. Mund të përfshijë uebfaqe që kopjojnë shumicën e përmbajtjes së tyre nga sajte të tjera, dhe fusin vetëm artikuj të rastësishëm partiak, polemik ose mashtrues. Mund të përfshijë shumë faktorë të tillë: Sfida për hulumtuesin është të identifikojë një kombinim tiparesh që i lejon për të thënë: "Ky aset është pjesë e këtij operacioni".



Modelet e sjelljes: Një artikull i postuar fillimisht në uebfaqen e Ajatollah Khameneit të Iranit, e më pas e riprodhuar pa atribuim nga IUVMpress.com dhe britishleft.com, dy uebfaqe në një rrjet propagandistik iranian. Imazhi nga DFRLab.

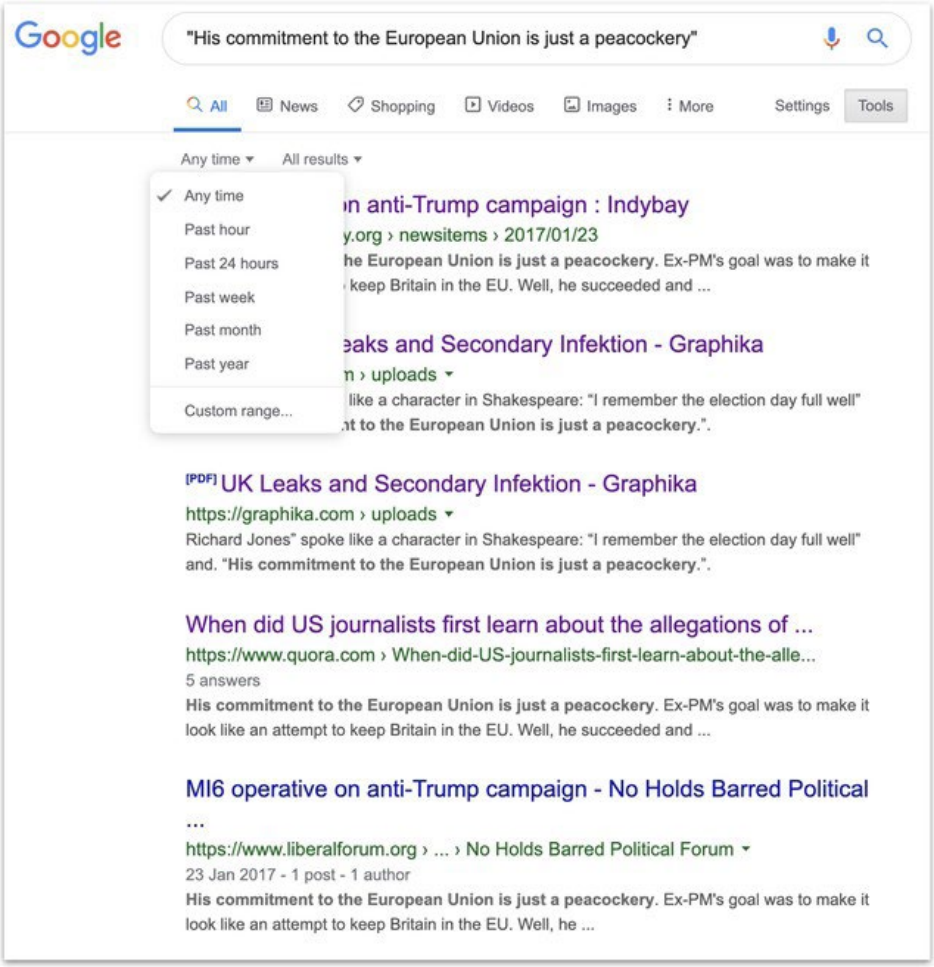
Ndonjëherë, mungesa e veçorive identifikuese mund të jetë në vetvete një tipar identifikues. Ky ishte rasti me fushatën "Infektimi sekondar" i drejtuar nga Rusia. Ajo përdorte qindra llogari në platforma të ndryshme bllogjesh, të cilat përfshinin detaje minimale biografike, postonin një artikull në ditën kur janë krijuar dhe më pas braktiseshin për të mos u përdorur më. Ky model sjelljeje ishte aq i përsëritur në kaq shumë llogari, sa u bë e qartë gjatë hetimit se ky ishte nënshkrimi i operacionit. Kur llogaritë anonime filluan të qarkullojnë dokumente tregtare mes SHBA dhe Mbretërisë së Bashkuar të zbuluara pak para zgjedhjeve të përgjithshme britanike të dhjetorit 2019, Graphika dhe Reuters treguan se ato përputheshin saktësisht me atë nënshkrim. Reddit e konfirmoi analizën.



Profili i Reddit për një llogari të quajtur "McDownes", që Reddit ia atribuon operacionit rus "Infektimi sekondar". Llogaria u krijua më 28 mars 2019, postoi një artikull pak më shumë se një minutë pasi u krijua dhe më pas ra në heshtje. Imazhi nga Graphika, të dhëna nga redective.com.

Të dhënat e përmbajtjes mund të ndihmojnë gjithashtu për të identifikuar asetet që janë pjesë e të njëjtit rrjet. Nëse një aset i njohur ndan një foto ose meme, ia vlen të kërkoni përsëri imazhin për të parë se ku tjetër është përdorur. Shtojca (plug-in) RevEye për ueb-shfletuesit është një mjet veçanërisht i dobishëm, pasi lejon hulumtuesit të ndryshojnë kërkimin përmes Google, Yandex, TinEye, Baidu dhe Bing. Gjithmonë ia vlen të përdorni shfletues të shumtë, pasi ata shpesh ofrojnë rezultate të ndryshme.

Nëse një aset shpërndan një tekst, ia vlen të kërkoni ku tjetër është shfaqur ai tekst. Sidomos me tekste më të gjata, këshillohet të zgjidhni një ose dy fjali nga paragrafët e tretë ose të katërt, ose më poshtë, pasi operacionet mashtruese janë të njohura për të redaktuar titujt dhe tekstet e artikujve që ata kanë kopjuar, por ka më pak gjasa që të marrin kohë për të redaktuar trupin e tekstit. Futja e seksionit të zgjedhur në thonjëza në një kërkim në Google do të kthejë përputhjen e saktë. Menyja "tools" (mjete) gjithashtu mund të klasifikojë çdo rezultat sipas datës.



Rezultatet e një kërkimi në Google për një frazë të postuar nga një operacion i dyshuar rus, që tregon funksionalitetin e veglave të Google për të kufizuar datën e kërkimit.

Asetet që postojnë tekst me gabime kanë vlerë të veçantë, pasi gabimet janë, për nga natyra e tyre, më të pazakonta se fjalët e shkruara saktë. Për shembull, një artikull nga një operacion i dyshuar i zbulimit rus i referohej Salisbury, qytetit britanik ku u helmua ish-agjenti rus Sergei Skripal, si "Solsbury". Kjo bëri një kërkim shumë më të synuar në Google me shumë më pak rezultate, sesa një kërkim për "Skripal" dhe "Salisbury". Prandaj, prodhoi një proporcion shumë më të lartë të gjetjeve të rëndësishme.

Me gjurmët për përmbajtjen, është veçanërisht e rëndësishme të shikoni tregues të tjerë, të tillë si modelet e sjelljes, për të konfirmuar nëse një aset i përket një operacioni. Ka shumë arsye legjitime që përdoruesit e paqëllimshëm të shpërndajnë përmbajtje nga operacionet e informacionit. Kjo do të thotë se shpërndarja e përmbajtjes nga një operacion është një sinjal i dobët. Për shembull, shumë përdorues kanë shpërndarë meme nga Agjencia Ruse e kërkimeve në internet, sepse ato meme kishin cilësi të vërteta virale. Shpërndarja e thjeshtë e përmbajtjes nuk mjafton në vete për të shënuar një aset si aset operacional.

Mbledhja e provave

Operacionet e informacionit dhe ndikimit janë të ndërlikuara dhe lëvizin shpejt. Një nga përvojat më zhgënjyese për një studiues të burimeve të hapura është të shohë një koleksion asetesh të hequra oflajn në gjysmë të rrugës së një hulumtimi. Prandaj, një rregull kyç i analizës është t'i regjistroni (incizoni) ato kur t'i gjeni, sepse mund të mos keni një shans të dytë.

Studiues të ndryshëm kanë preferenca të ndryshme për regjistrimin (ruajtjen) e aseteve që gjejnë, e nevojat ndryshojnë nga operacioni në operacion. Fletëllogaritëset apo tabelat (spreadsheets) janë të dobishme për regjistrimin e informacionit bazë për një numër të madh të aseteve; Dosjet e përbashkëta të bazuara në re kompjuterike (clouds) janë të dobishme për ruajtjen e një numri të madh skrinshotesh (nëse kërkohen skrinshote, është jetike që fajlit t'i jepet

menjëherë emri i identifikueshëm: pak gjëra janë më të bezdisshme sesa të përpiqesh të gjesh se cili nga 100 fajlet e quajtur "Screenshot" është ai që ju nevojitet). Dokumentet tekstuale janë të mira për të regjistruar një përzierje informacioni, por shpejt bëhen të rrëmujshme dhe të ngathëta nëse operacioni është i madh.

Cilido qoftë formati, disa informacione duhet të regjistrohen gjithmonë. Këto përfshijnë mënyrën se si është gjetur aseti (një pikë thelbësore), emrin dhe URL-në e tij, datën e krijimit (nëse dihet) dhe numrin e ndjekësve, ata që ai i ndjek, pëlqimeve dhe/ose shikimeve. Ato përfshijnë gjithashtu një përshkrim bazë të asetit (për shembull, "Llogaria pro-saudite në gjuhën arabe me fotografinë e profilit të Ema Uotson"), për t'ju kujtuar se çfarë ishte pasi të shikoni 500 asete të tjera. Nëse punoni në një ekip, ia vlen të regjistroni se cili anëtar i ekipit ka shikuar cilin aset.

Linqet mund të ruhen duke përdorur një shërbim arkivimi si Wayback Machine ose archive.is, por keni kujdes që arkivat të mos ekspozojnë përdoruesit e vërtetë që mund të kenë ndërvepruar padashur me asetet e dyshimta dhe sigurohuni që linku i arkivit ruan pamjet vizuale, ose bëni një skrinshot si rezervë. Sigurohuni që të gjitha asetet të ruhen në vende të mbrojtura, të tilla si fajle të mbrojtura me fjalëkalim ose kasaforta të enkriptuara. Mbani gjurmët se kush ka qasje dhe rishikoni rregullisht qasjen.

Së fundi, ia vlen t'i jepet asetit një vlerësim besimi. Operacionet e ndikimit shpesh gjejnë përdorues të paqëllimshëm për të amplifikuar përmbajtjen e tyre: në të vërtetë, kjo është shpesh qëllimi. Sa i sigurt jeni që aseti më i fundit është pjesë e këtij operacioni dhe pse? Niveli i besimit (i lartë, i moderuar ose i ulët) duhet të shënohet si një hyrje më vete dhe arsyet (të diskutuara më poshtë) duhet t'u shtohen shënimeve.

Atribuimi dhe besimi

Sfida më e madhe në identifikimin e një operacioni të informacionit qëndron në atribuimin e tij te një aktor specifik. Në shumë raste, atribuimi i saktë do të jetë përtej mundësive të hulumtuesve të burimeve të hapura. Më e mira që mund të arrihet është një shkallë e besimit se një operacion ndoshta drejtohet nga një aktor i caktuar, ose se asete të ndryshme i përkasin një operacioni specifik, por përcaktimi se kush qëndron pas operacionit është rrallë i mundshëm me burime të hapura.

Informacione të tilla si regjistrimet në ueb, adresat IP dhe numrat e telefonit mund të ofrojnë një atribuim të fortë, por ato shpesh maskohen për të gjithë, përveç se për platformat e mediave sociale. Prandaj kontaktimi me platformat relevante është një pjesë jetike e punës hetimore. Ndërsa platformat kanë rritur ekipet e tyre të brendshme hetimore, ato janë bërë më të gatshme për të ofruar atribuime publike për operacionet e informacionit. Atribuimi më i fortë në rastet e fundit ka ardhur drejtpërdrejt nga platformat, si ekspozimi që ua bën Twitter-i operacioneve të informacionit të mbështetura nga shteti kinez që synojnë Hong Kongun, si dhe ekspozimi që ua bën Facebook-u operacioneve të lidhura me qeverinë saudite.

Gjurmët nga përmbajtja mund të luajnë një rol. Për shembull, një operacion i ekspozuar në Instagram në tetor të vitit 2019 postoi meme që ishin pothuajse identike me meme-t e postuara nga Agjencia Ruse e kërkimeve në internet, por pa vulat e shënjimit (watermark) të IRA-s. E vetmja mënyrë që ata mund t'i bënin këto meme ishte të siguronin imazhet origjinale që ishin bazë për postimet e IFIA, e më pas të rindërtonin meme-t mbi to. Për ironi, kjo përpjekje për të maskuar origjinën e postimeve të IRA-s sugjeroi se krijuesit ishin, në fakt, vetë IRA.

Ngjashëm me këtë, një rrjet i madh uebfaqesh në dukje të pavarura postoi vazhdimisht artikuj që ishin kopjuar, pa atribuim, nga burime të qeverisë iraniane. Ky model ishte aq i përsëritur sa doli të ishte aktiviteti kryesor i uebfaqeve. Si i tillë, ishte e mundur që ky operacion t'i atribuohej aktorëve pro-iranianë, por nuk ishte e mundur t'i atribuohej më tej vetë qeverisë iraniane.

Në fund të fundit, atribuimi është një çështje e vetëpërmbajtjes. Hulumtuesi duhet të imagjinojë pyetjen: "Si mund të dëshmoni se ky operacion është drejtuar nga personi që po akuzoni?" Nëse ata nuk mund t'i përgjigjen kësaj pyetjeje që ia bëjnë vetes me vetëbesim, atëherë duhet të shmangin nga bërja e akuzës. Identifikimi dhe ekspozimi i një operacioni të informacionit është punë e vështirë dhe e rëndësishme, dhe bërja e një atribuimi të pambështetur ose të pasaktë mund të dëmtojë gjithçka që ka ardhur përpara tij.

11a. Rast studimi: Atribuimi i rastit Endless Mayfly (miza pafund)

Shkruan: Gabriele Lim

Gabriele Lim *(Gabrielle Lim) është një studiuese në Projektin Kërkimor të Teknologjisë dhe Ndryshimeve Sociale në Qendrën Shorenstein të Shkollës Kennedy të Harvardit dhe bashkëpunëtore me Citizen Lab. Ajo studion implikimet e censurës dhe manipulimit mediatik mbi sigurinë dhe të drejtat e njeriut.*

Në prill të vitit 2017, një artikull joautentik që aktronte në mënyrë mashtruese gazetën britanike The Independent u postua në Reddit. Ky artikull citonte në mënyrë të rreme ish-zëvendëskryeministrin e Mbretërisë së Bashkuar, Nik Kleg (Nick Clegg), se gjoja thoshte se kryeministrja e atëhershme Tereza Mej (Theresa May) po "u puthte dorë regjimeve arabe". Reddit-orët e zgjuar nxituan ta quanin postimin si të dyshimtë dhe të rremë. Jo vetëm që ishte hostuar në indepnedent.co në krahasim me www.independent.co.uk , por postuesi origjinal ishte një personazh i cekët që kishte postuar gjithashtu disa artikuj të tjerë joautentikë në Reddit.

Nga ai artikull fillestar, domen dhe personazh që ishin joautentik, studiuesit në Citizen Lab shpenzuan 22 muajt e ardhshëm duke gjurmuar dhe hetuar rrjetin pas këtij operacioni të shumëanshëm të informacionit onlajn. I quajtur Endless Mayfly (miza pafund), qëllimi i operacionit ishte të targetonte gazetarët dhe aktivistët me uebfaqe joautentike që pretendonin rrejshëm se janë uebfaqe të mediave të etabluara, dhe duke shpërndarë informacione të rreme dhe përçarëse.

Thënë në përgjithësi, rrjeti bënte mashtrim duke u prezantuar si media e lajmeve me reputacion me një artikull joautentik, e amplifikonte atë nëpërmjet një rrjeti uebfaqesh dhe personash të rremë në Twitter dhe më pas ose do ta fshinte ose do ta ridrejtonte artikullin joautentik, pasi të krijohej një zhurmë në internet. Më poshtë është një shembull i një artikulli të falsifikuar që u maskua si Bloomberg.com duke shkruar bloomberq.com qëllimisht me gabim (typosquatting):

Ky imazh tregon dy persona të rremë onlajn të lidhur me Endless Mayfly, duke tuituar një link të versioni-kopje e Daily Sabah, një gazetë turke. Vini re se personi në të djathtë, "jolie prevoit", po përdor një foto të aktores Elisha Kathbert si foto profili.

Deri në kohën kur publikuam raportin tonë në maj 2019, grupi ynë i të dhënave përfshinte 135 artikuj joautentikë, 72 domene, 11 persona, një organizatë të rreme dhe një rrjet botues pro-Iranian që amplifikonte të pavërtetat e gjetura në artikujt joautentikë. Në fund, konkluduam me vetëbesim të moderuar se Endless Mayfly ishte një operacion informacioni i afërt me Iranin.

Endless Mayfly ilustron se si mund të kombinoni analizën e rrjetit dhe narrativës me raportimin e jashtëm për të arritur deri në atribuim. Rasti gjithashtu thekson vështirësinë e përfshirë në atribuimin e operacioneve të informacionit te një aktor specifik, pse nevojiten tregues të shumëfishtë dhe si të përdoret një nivel besimi për të treguar nivelin tuaj të sigurisë për atribuimin.

Në fund të fundit, atribuimi është një detyrë e vështirë shpesh e kufizuar nga informacioni i papërsosur, përveç nëse jeni në gjendje të nxirrni një pranim ose të siguroni provë përfundimtare. Kjo është arsyeja pse atribuimi shpesh shprehet si një vlerësim probabilist në shumë raste të manipulimit të medias.

Triangulimi i pikave të shumta të të dhënave dhe analizave

Për shkak të natyrës klandestine të operacioneve të informacionit, aftësisë së aktorëve për t'u përfshirë në fushata të "flamurit të rremë" dhe natyrës kalimtare të dëshmive, atribuimi duhet të jetë rezultat i një kombinimi analizash dhe provash. Me Endless Mayfly, ne përfunduam me besim të moderuar se ishte një operacion i afërt me Iranin për shkak të treguesve që rrjedhin nga tre lloje analizash:

1. Analiza e narrativave
2. Analiza e rrjetit
3. Raportimi dhe analiza e jashtme

1. Analiza e narrativave

Duke përdorur analizën e përmbajtjes dhe të diskursit mbi 135 artikujt joautentikë të mbledhur në hetimin tonë, përcaktuam se narrativat që po përhapeshin ishin në përputhje me interesat e Iranit. Çdo artikull u kodua në kategori që u përcaktuan pas një leximi fillestar të të gjithë artikujve. U kryen dy raunde kodimi: Raundi i parë u ekzekutua në mënyrë të pavarur nga dy studiues dhe një raund i dytë u krye së bashku nga të njëjtët studiues për të zgjidhur çdo mospërputhje. Kjo tabelë paraqet rezultatet e procesit tonë të kodimit.

Kategoria	Numri i artikujve	Përshkrim i kategorisë
Mosmarrëveshje gjeopolitike	63 [46.7%]	Artikulli përshkruan ngjarje, veprime ose deklarata të bëra nga zyrtarë qeveritarë ndaj një shteti të huaj që mund të interpretohen si provokuese, armiqësore ose në kundërshtim me interesat e shtetit të huaj.
Mosmarrëveshje e brendshme	16 (11.9%)	Artikulli përshkruan ngjarje, veprime ose deklarata të bëra nga aktorë politikë që mund të mbjellin përçarje midis partive politike ose aktorëve brenda të njëjtit shtet.
Bashkëpunim me Izraelin	14 (10.4%)	Artikulli përshkruan ngjarje, veprime ose deklarata të bëra nga aktorë politikë ose zyrtarë qeveritarë që tregojnë bashkëpunim midis Izraelit dhe një shteti tjetër.
Arabia Saudite përkrah terrorizmin	9 (6.7%)	Artikulli përshkruan ngjarje, veprime ose deklarata të bëra nga aktorë politikë ose zyrtarë qeveritarë që tregojnë bashkëpunim midis Izraelit dhe një shteti tjetër.
Të tjera	5 (3.7%)	Artikulli nuk bën pjesë në asnjë nga kategoritë.
Nuk ka arkiv	31 (23%)	Artikulli nuk mund të kodohet sepse nuk ekziston më dhe nuk ka cache, skrinshot ose kopje të tekstit për të kryer ndonjë analizë kuptimplotë.
Kopje e artikullit ekzistues	5 (3.7%)	Artikulli është një kopjim/ngjitje (copy-paste) e drejtpërdrejtë e një artikulli të vërtetë ekzistues.

Pasi u koduan të gjithë artikujt, ishim në gjendje të përcaktonim narrativat më të zakonshëm të propaguara nga Endless Mayfly. I krahasuam këto me kërkimin tonë paraprak mbi rajonin. Kjo përfshinte hulumtim të zgjeruar për të kuptuar rivalitetet dhe aleancat e rajonit, interesat dhe kërcënimet gjeopolitike dhe historinë e kontrolleve të informacionit. Kjo ishte e nevojshme që ne të kontekstualizonim provat dhe t'i vendosim narrativat në kontekstin më të gjerë politik. Me rezultatet e kodimit në dorë, përcaktuam se këto narrativa me shumë gjasa po i shërbenin interesave të Iranit.

2. Analiza e rrjetit

Analiza e rrjetit u krye për të përcaktuar se cilat domene ose platforma ishin përgjegjëse për amplifikimin e përmbajtjes. Për Endless Mayfly, dy rrjete ishin të përfshira në shpërndarjen e artikujve joautentikë dhe të pavërtetave të tyre: një rrjet uebfaqesh pro-Iraniane dhe një grup personash pro-Iranianë në Twitter. Të dyja u bënë faktor në atribuimin e Endless Mayfly, sepse ata vazhdimisht shtynin storie që ishin në përputhje me politikat zyrtare iraniane, deklaratat publike dhe qëndrimet në lidhje me Arabinë Saudite, Izraelin dhe Shtetet e Bashkuara.

Rrjeti botues — Rrjeti botues përbëhej nga një numër faqesh interneti në dukje pro Iranit që e portretizonin veten si media të pavarura të lajmeve. Në total, ne gjetëm 353 uebfaqe në 132 domene që u referoheshin ose lidheshin me artikujt joautentikë të Endless Mayfly. Ky proces përfshinte një kërkim në Google për të gjitha URL-të e artikujve joautentikë dhe titujt e tyre. Përveç kësaj, ne skanuam linqet e tuituara nga personat në rrjetin tonë, duke identifikuar uebfaqet që përmbanin referenca ose linqe me artikujt.

Pas këtij procesi, identifikuam 10 domenet kryesore që u referoheshin më shpesh artikujve joautentikë. Nga këto 10 domene, 8 ndanin të njëjtën adresë IP ose detaje të regjistrimit, që jepte indikacion se ato mund të kontrollohen nga i njëjti aktor. Përmbajtja e këtyre faqeve gjithashtu anonte drejt promovimit të interesave iraniane. Për shembull, IUVM Press, e cila bënte linqe ose iu referohej artikujve joautentikë të Endless Mayfly 57 herë, hostoi një dokument PDF të titulluar "Statut" që shprehte qartë se ata ishin kundër "aktiviteteve dhe projekteve të shteteve të arrogancës globale, imperializmit dhe sionizmit" dhe se "Selia e Unionit ndodhet në Teheran - kryeqyteti i Republikës Islamike të Iranit."

Rrjeti i personave — Ngjashëm me artikujt joautentikë dhe rrjetin botues, personat e lidhur me Endless Mayfly në Twitter ishin me vendosmëri kritikë ndaj Arabisë Saudite, Izraelit dhe kombeve perëndimore në përgjithësi. Një analizë e aktivitetit të tyre në Twitter zbuloi se këto llogari shtynin një kombinim artikujsh të besueshëm dhe joautentikë që ishin shumë kritikë ndaj rivalëve politikë të Iranit. Merrni, për shembull, llogarinë në Twitter për "Komunitetin e paqes, sigurisë, drejtësisë" (Peace, Security, Justice Community), një organizatë e rreme e identifikuar nga hetimi ynë, i paraqitur më poshtë. Jo vetëm që propagandonte përmbajtje që ishte kundër Arabisë Saudite, Izraelit dhe SHBA-së, por edhe fotografia e profilit dhe imazhi i header-it gjithashtu vinin në shënjestër Arabinë Saudite. Vini re shenjën e shënjestrës mbi Arabinë Saudite në foton e profilit dhe hartën e përdorur në header (imazhin në krye të profilit). Biografia e llogarisë gjithashtu thekson në mënyrë eksplicite Arabinë Saudite dhe ideologjinë vehabiste si shkaktar të ekstremizmit.

Në mënyrë të ngjashme, ky postim në Twitter nga një personazh tjetër i Endless Mayfly, "Mona A. Rahman", përmend gazetarin dhe kritikun saudit Ali al-Ahmed ndërsa kritikon princin e kurorës së Arabisë Saudite, Mohammad bin Salman.

3. Raportimi dhe analiza e jashtme

Gjithashtu, i krahasuam gjetjet dhe të dhënat tona me raportimin e jashtëm. Duke ndjekur një këshillë nga FireEye në gusht 2018, për shembull, Facebook çaktivizoi disa llogari dhe faqe të lidhura me rrjetin publikues të përdorur nga Endless Mayfly. Në analizën që bëri, FireEye identifikoi disa domene që ishin pjesë e rrjetit publikues që kishim identifikuar, si institutomanquehue.org dhe RPFront.com. Ashtu si ne, ata gjithashtu konkluduan me besim të moderuar se "operacioni i dyshuar i ndikimit" duket se e ka origjinën nga Irani. Facebook-u, në njoftimin që dha, në mënyrë të ngjashme vuri në dukje se operacionet ka shumë të ngjarë të kenë pasur origjinën nga Irani.

Përveç kësaj, Twitter publikoi një grup të dhënash të llogarive të lidhura me Iranin që ishin pezulluar për "manipulim të koordinuar". Megjithëse llogaritë me më pak se 5000 ndjekës në kohën e pezullimit ishin anonime, ishim në gjendje të identifikonim një personazh të Endless Mayfly (@Shammari_Tariq) në grupin e të dhënave të Twitter-it.

Vlerësimet nga Twitter-i, Facebook-u dhe FireEye ishin të dobishme për të vërtetuar hipotezën tonë, sepse ato nxorën në sipërfaqe prova që nuk ishin pjesë e përpjekjeve tona për mbledhjen e të dhënave dhe mbi-përputheshin me asetet e Endless Mayfly që identifikuam ne. Për shembull, analiza e FireEye identifikoi numrat e telefonit dhe informacionin e regjistrimit të lidhur me llogaritë në Twitter dhe domenet e lidhura me Endless Mayfly - dëshmi që nuk ishte pjesë e të dhënave tona. Po kështu, Facebook-u dhe Twitter-i me sa duket kishin informacione për regjistrimin e llogarisë, të tilla si adresat IP, në të cilat ne nuk kemi qasje. Prandaj, pikat shtesë të të dhënave të identifikuara nga këto raporte të jashtme ndihmuan në zgjerimin e trupit të provave.

Arritja te besimi i moderuar

Në rastin e Endless Mayfly, provat që mblodhëm - narrativat, personat dhe rrjeti botues pro-Iranian, treguan Iranin si një burim të besueshëm të operacionit të informacionit. Ky grup provash më pas u krahasua me raportimet dhe hulumtimet e jashtme të besueshme nga FireEye, Facebook dhe Twitter, të cilat vërtetuan gjetjet tona. Çdo provë individuale, ndonëse e pamjaftueshme më vete për atribuim, ndihmoi në konfirmimin dhe forcimin e hipotezës sonë kur u vlerësua në mënyrë holistike dhe kur krahasohej me tërësinë e dëshmive që i shpërfaqi hetimi ynë.

Pavarësisht nga treguesit e shumtë që tregojnë drejt Iranit, ne ende nuk kishim prova përfundimtare. Prandaj, e përdorëm një kornizë të atribuimit kibernetik që është e zakonshme brenda komunitetit të zbulimit. Ai përdor tregues të shumëfishtë dhe besim probabilistik (i ulët, i moderuar, i lartë), duke u lejuar hulumtuesve të përcjellin gjetjet e tyre duke e kualifikuar nivelin e tyre të pasigurisë.

Përfundimisht, ne arritëm në përfundimin se Endless Mayfly është një operacion i lidhur me Iranin me besim të moderuar, të cilin Zyra e Drejtorit të Zbulimit Kombëtar të SHBA-së e përcakton që do të thotë se "informacioni është me burim të besueshëm dhe i mundshëm, por jo i cilësisë së mjaftueshme ose i vërtetuar mjaftueshëm për të garantuar një nivel më të lartë të besimit". Ne nuk zgjodhëm një nivel më të lartë besimi, sepse menduam se nuk kishte prova të mjaftueshme për të përjashtuar plotësisht një operacion të "flamurit të rremë" - që do të thotë se dikush përpiqet ta bëjë të duket sikur Irani ishte pas këtij operacioni - ose një palë e tretë që ka simpati për interesat iraniane.

Atribuimi i operacioneve të informacionit si Endless Mayfly do të mbështetet pothuajse gjithmonë në informacione jo të plota dhe të papërsosura. Prandaj, bashkëngjitja e niveleve të besimit me gjetjet është një komponent i rëndësishëm i atribuimit - pasi funksionon me një kujdes të bollshëm. Atribuimi i gabuar ose niveli i rritur i besimit mund të ketë pasoja të tmerrshme, veçanërisht nëse politikat e qeverisë dhe masat hakmarrëse rezultojnë nga ky vlerësim i gabuar. Për të shmangur praktikat e nxituara dhe të dobëta të atribuimit, është e rëndësishme të merren parasysh tregues të shumtë, lloje të provave dhe analizave, dhe të përdoret një nivel besimi që merr parasysh hipotezat alternative dhe të dhënat që mungojnë.

11b. Rast studimi: Hetimi i një operacioni të informacionit në Papuan Perëndimore

Shkruajnë: Eliz Tomas , Benxhamin Strik

Benxhamin Strik *(Benjamin Strick) është një hetues i burimeve të hapura për BBC, kontribues i Bellingcat dhe instruktor në teknikat me burim të hapur, zbulimin gjeohapësinor dhe analizën e rrjeteve. Ai ka përvojë në drejtësi dhe ushtri, dhe fokusohet në përdorimin e metodave OSINT/GEOINT, gjeolokimit dhe metodave të zbulimit për qëllime të mira, përmes të drejtave të njeriut, konfliktit dhe privatësisë.*

Eliz tomas *(Elise Thomas) është gazetare e pavarur dhe hulumtuese që punon me Qendrën Ndërkombëtare të Politikave Kibernetike në Institutin Australian të Politikave Strategjike. Shkrimet e saja janë botuar në Wired, Foreign Policy, The Daily Beast, The Guardian dhe media tjera. Ajo gjithashtu ka punuar më parë si asistente redaktuese për Zyrën e OKB për Koordinimin e Çështjeve Humanitare dhe si shkrimtare dhe studiuese e podkasteve.*

Në gusht të vitit 2019, tensionet separatiste u ndezën përsëri në Papuan Perëndimore, një provincë që u bë pjesë e Indonezisë me një vendim të diskutueshëm në vitet e gjashtëdhjeta të shekullit të kaluar. Që atëherë, rajoni ka vuajtur nga pretendimet e përhapura për abuzime të të drejtave të njeriut të kryera nga autoritetet indoneziane për të shuar mospajtimin.

Qasja në rajon është shumë e kufizuar dhe gazetarëve të huaj u është ndaluar të raportojnë në provincë. E gjithë kjo i bën mediat sociale një burim thelbësor për monitorimin dhe raportimin për Papuan Perëndimore.

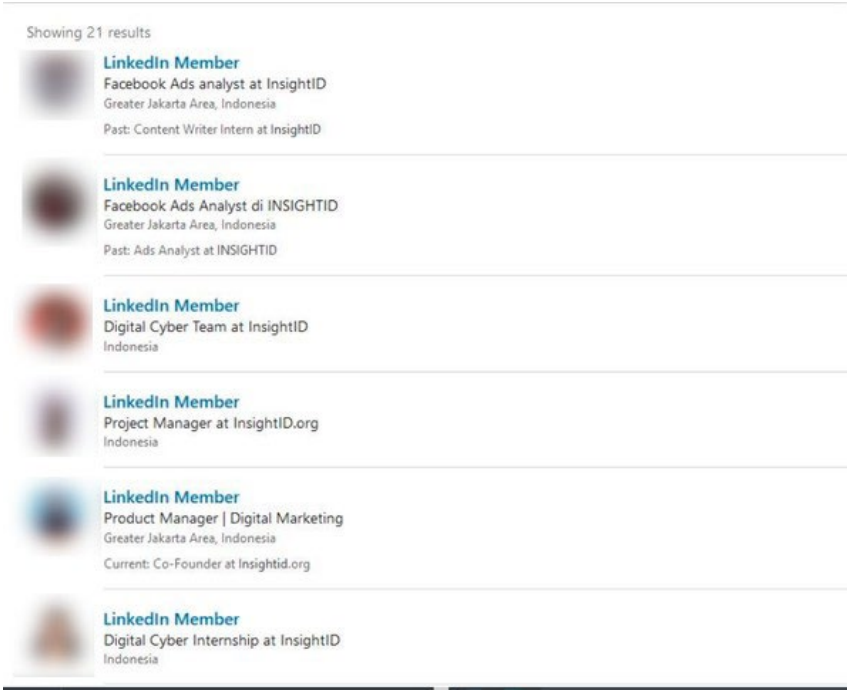
Ndërsa përpiqej të gjeo-lokonte disa nga pamjet që po dilnin nga dhuna në FakFak, njëri prej nesh identifikoi dy hashtagje të përhapur në Twitter, #WestPapua dhe #FreeWestPapua.

Kërkimet me ato hashtagje zbuluan një valë llogarish të rreme që postonin automatikisht të njëjtat video dhe të njëjtin tekst duke përdorur të njëjtat hashtagje. Llogaritë gjithashtu rituitonin dhe pëlqenin përmbajtjen e njëra-tjetrës, duke ndihmuar në amplifikimin e mëtejshëm të saj dhe rritjen e angazhimit në hashtagje.

Procesi për analizimin e këtyre llogarive të automatizuara u detajua në Kapitullin 3. Duke u mbështetur në atë punë, ne zgjeruam hetimin tonë duke punuar për të identifikuar njerëzit ose grupet prapa operacioneve. Gjatë procesit, zbuluam një fushatë të ngjashme, më të vogël dhe në dukje të palidhur, dhe mundëm të identifikonim edhe individin përgjegjës. Operatorët e të dy fushatave më në fund e pranuan përfshirjen e tyre pasi u kontaktuan nga BBC.

Madhësia e fushatës së parë dhe fakti që ajo po operonte në platforma të shumta na dhanë një sërë mundësish për të gjetur të dhëna që mund t'i përdorim për t'u fokusuar për të gjetur më shumë informacion rreth operatorëve të fushatës.

Informacioni i parë i dobishëm ishin uebfaqet që shpërndaheshin nga rrjeti i llogarive në Twitter dhe Facebook. Kërkimet në Whois zbuluan se katër nga domenet ishin regjistruar duke përdorur një emër të rremë dhe një adresë e-maili false, por me një numër telefoni të vërtetë. Ne futëm numrin në WhatsApp për të parë nëse ishte i lidhur me një llogari. Ishte, dhe ajo llogari kishte gjithashtu një foto profili. Duke përdorur kërkimin e kundërt të imazhit Yandex për atë foto të profilit, arritëm ta lidhnim foton e profilit me llogaritë në Facebook, LinkedIn dhe Freelancer.com. Nëpërmjet asaj llogarie të lidhur në LinkedIn, ishim në gjendje të gjenim vendin aktual të punës të personit dhe të shihnim kolegët e tij.



Individi ishte një punonjës i një kompanie me bazë në Xhakartë e quajtur InsightID, në faqen e së cilës thuhej se ofronte "programe të integruara të PR-it dhe marketingut digjital".

Gjithashtu mblodhëm pika shtesë të të dhënave se InsightID ishte përgjegjëse rreth operacionit të informacionit. Në uebfaqen e saj, InsightID iu referua punës së saj në "Nismën e programit për zhvillimit të Papuas" (Papua Program Development Initiative), e cila "ekzaminon zhvillimin e shpejtë socio-ekonomik të Papuas dhe hulumton sfidat e tij". Ish-nëpunësit dhe praktikantët e InsightID përshkruan se kanë prodhuar përmbajtje video, kanë redaktuar dhe kanë përkthyer përmbajtje si pjesë e punës së tyre në Projektin e Zhvillimit të Papuas.

Një ish-nëpunës deklaroi në profilin e tyre në LinkedIn se puna e tyre mund të shihej në "West Papuan (Instagram, Facebook, Website)". West Papuan ishte një nga pesë uebfaqet e lajmeve të përfshira në fushatë. Një tjetër punonjës i InsightID krijoi një llogari në YouTube në emrin e tij për të hostuar një video si pjesë e fushatës. Kjo video më pas u fut (embedua) në westpapuan.org.

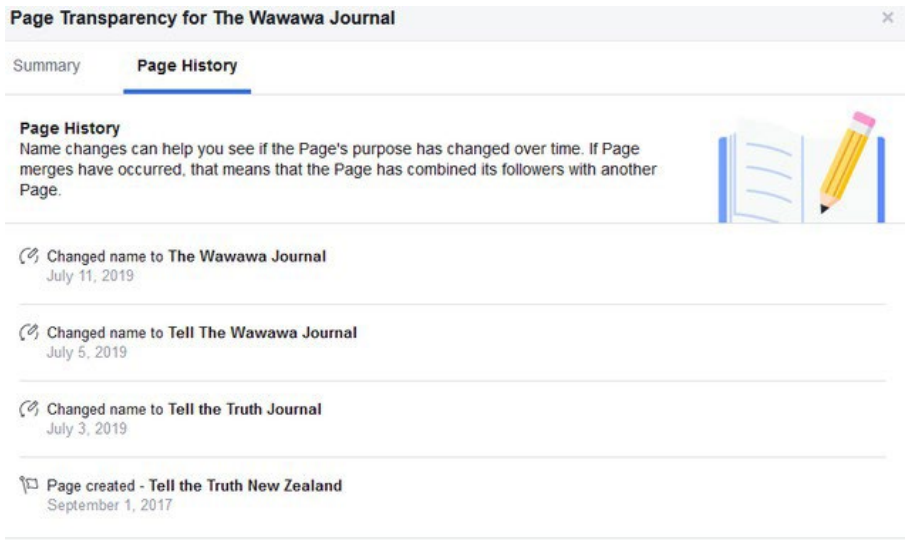
Kërkimet e mëtejshme të regjistrimeve të domenit zbuluan se bashkëthemeluesi i InsightID ka përdorur adresën e e-mailit të kompanisë së tij për të regjistruar 14 domene në të njëjtën ditë, shumica e të cilave lidheshin drejtpërdrejt me Papuan Perëndimore. Këto përfshinin westpapuafreedom.com, westpapuagenocide.com dhe westpapuafact.com. Çdo informacion shtesë i shtohej provave se InsightID ishte përgjegjës për operacionin.

Në atë moment, gazetarët e BBC u përpoqën të kontaktojnë InsightID për koment. Megjithëse kompania nuk u përgjigj, InsightID përfundimisht pranoi përgjegjësinë e saj, duke thënë në një postim në mediat sociale se "përmbajtja jonë mbron Indonezinë kundër narrativës mashtruese të grupeve separatiste të Papua-s së Lirë".

Ne nuk ishim në gjendje të identifikonim klientin që ka kontraktuar InsightID për të kryer fushatën e informacionit.

Ndërsa zbulonim këtë operacion më të madh, hetuam gjithashtu një rrjet më të vogël prej tre uebfaqesh që maskoheshin si burime të pavarura lajmesh dhe kishin profile të lidhura në mediat sociale. Edhe pse në dukje nuk ishin të lidhura me fushatën e parë, këto faqe synonin perceptimet ndërkombëtare të situatës në Papuan Perëndimore, duke u fokusuar te audienca në Zelandën e Re dhe Australi.

Ajo që ishte kyçe për identifikimin e individit përgjegjës ishte se faqja në Facebook për një markë (brend), Wawawa Journal, fillimisht quhej Tell the Truth NZ. Ne ishim në gjendje ta shihnim këtë duke parë historinë e emërtimit të faqes. Kjo na lejoi ta lidhnim përsëri me domenin tellthetruthnz.com, i cili ishte regjistruar te Muhamad Rosyid Jazuli.



Kur iu qasën gazetarët e BBC-së, Jazuli pranoi se ishte operatori i fushatës. Ai punon me Qendrën Jenggala, një organizatë e krijuar nga nënpresidenti i Indonezisë, Jusuf Kalla. Ajo është krijuar në vitin 2014 për të promovuar rizgjedhjen e tij dhe për të mbështetur administratën e Presidentit Jokovi.

Ajo që tregon ky hulumtim është se identifikimi i fushatave informuese dhe atribuimi i tyre tek individët dhe grupet përgjegjëse nuk kërkon domosdoshmërisht teknika apo mjete të komplikuara – por kërkon durim dhe një sasi të caktuar fati. Ky hetim u mbështet në resurse me burim të hapur, si regjistrimet e Whois, kërkimi i kundërt i imazheve, profilet e mediave sociale dhe analiza e kodeve burimore të uebfaqeve. Fakti që fushata ishte në veprim në platforma të shumta, në kombinim me mediat sociale dhe profilet LinkedIn të punonjësve të InsightID, ishte vendimtar për të na lejuar të bashkonim shumë të dhëna të vogla për të ndërtuar pikturën më të madhe.

Nëse ka një mësim kyç për të marrë nga ky shembull, kjo është të mendoni se si mund të përdorni detaje ose të dhëna nga një platformë për t'u drejtuar kah një platformë tjetër.

Për botimin dhe autorët

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

Redaktor: **Kraig Silverman**

Redaktore kontribuese: **Claire Wardle**

Redaktore gjuhësore: **Merrill Perlman**

Autorë: **Ben Collins, Ben Nimmo, Benjamin Strick, Brandy Zadrozny, Charlotte Godart, Claire Wardle, Craig Silverman, Donie O'Sullivan, Elise Thomas, Farida Vis, Gabrielle Lim, Gemma Bagayaua-Mendoza, Hannah Guy, Henk van Ess, Jane Lytvynenko, Joan Donovan, Johanna Wild, Sam Gregory, Sergio Liidtke, Simon Faulkner, Vernise Tantuco**

Drejtues i produksionit: **Arne Grauls**

Përkthimi dhe përshtatja në gjuhën shqipe: **Petrit Saraçini**

Ky libër është botuar nga Qendra Evropiane e Gazetarisë dhe është bërë i mundur falë financimit nga Craig Newmark Philanthropies. Supported by