Laskennallinen propaganda -
Keinojen kartoitus ja käytön arviointi tapauskuvauksen kautta

Pietari Pikkuaho

Pro gradu -tutkielma

Valtio-oppi

Turun Yliopisto

Syyskuu 2020

TURUN YLIOPISTO
Filosofian, poliittisen historian ja valtio-opin laitos / Yhteiskuntatieteellinen tiedekunta

PIKKUAHO, PIETARI: Laskennallinen propaganda: Keinojen kartoitus ja käytön arviointi tapauskuvauksen kautta

Pro gradu -tutkielma 101 s., + liitteet 2s.
Valtio-oppi
Syyskuu 2020

Sosiaalisessa mediassa tapahtuva algoritmisavusteinen poliittinen manipulaatio, laskennallinen propaganda, on viimeisen kymmenen vuoden aikana muodostunut yhteiskunnallista turvallisuutta uhkaavaksi ongelmaksi. Valtiolliset, poliittiset ja kaupalliset toimijat hyödyntävät uudenlaisen sosiaalisen viestintämuodon tuomia mahdollisuuksia poliittisten, taloudellisten ja valtiollisten tavoitteiden saavuttamiseen. Informaatiosodankäynnin, poliittisen kamppailun ja perinteisen tuotemarkkinoinnin sähköistyessä lainsäädäntö ja toimitavat vastaavat puutteellisesti pahantahtoisten toimijoiden esittämiin haasteisiin ja jättävät yhteiskuntamme haavoittuvaisiksi hyökkäyksille. Tämä pro gradu – työ tarkastelee laskennallisen propagandan käyttöä, sitä käyttäviä toimijoita sekä näiden keinoja tapaus- ja keinokuvauksen kautta.

Tutkielma jaottelee toimijat kaupallisiin, poliittisiin ja valtiollisiin, sekä alustoihin. Yleinen toimijakuvaus alustaa tapauskuvauksia, jotka käsittelevät IRA:n ja Venäjän vaikutusoperaatioita sekä vaalisekaantumista vuoden 2016 Yhdysvaltain presidentinvaaleihin ja valtiolähtöistä disinformaatiota vuoden 2020 koronavirus-pandemian aikana. Tapauskuvausta tuetaan laskennallisen propagandan menetelmäesittelyllä, joka kuvaa keskeisiä laskennallisen propagandan menetelmiä ja käsitteitä.

Työn kautta esille nouseva ilmiön keskeinen haaste on alustojen läpinäkymättömyys. Yhteistyöstä kieltäytyminen lainsäätäjien ja tutkijoiden kanssa johtaa tilanteeseen jossa alustat päätyvät suojelemaan disinformatiivisia vaikutuskampanjoita suorittavia toimijoita sekä informaatiosodankäyntiin osallistuvia maita. Keskeisiä torjuntamenetelmiä ilmiölle pohjustaisikin suurempi yhteistyö ja läpinäkyvyys alustojen osalta.

Asiasanat: disinformaatio, misinformaatio, laskennallinen propaganda, alustat, sosiaalinen media, Covid19-pandemia, koronavirus-pandemia, vaikutusoperaatiot, sosiaalisen median manipulaatio, algoritminen manipulaatio, propaganda, Facebook, IRA, Kiina, Venäjä

Sisällysluettelo

1. Johdanto

Viimeinen vuosikymmen on nostanut laskennallisen propagandan ja sosiaalisen median kautta tapahtuvan poliittisen manipulaation julkiseen tietoisuuteen. Brexit, Yhdysvaltain 2016 presidentinvaalit, Cambridge, Analytica, Kiina, Venäjä, Iran, Brasilia. Disinformaatio, botit, valeuutiset, mikrokohdennetut mainokset.

Nämä termit ovat pyörineet uutissyklissä erityisesti viimeisen viiden vuoden aikana. Pelot vieraista toimijoista sekä yrityksistä, jotka käyttävät sosiaalisen median alustoja kaapatakseen demokratiamme ovat nousseet tietoisuuteen.

Mutta miten nämä toimijat aikovat kaapata demokratiamme? Mikä mahdollistaa vieraan vallan agenteille vaalien kääntämisen kotimaassamme ja mitä keinoja ne käyttävät?

Tutkimuskirjallisuudessa paras määritelmä näille keinoille on ollut laskennallisen propagandan määritelmä.[1] Laskennallinen propaganda on sekä ilmiö, termi että nouseva tutkimusala. Se tutkii laajasti sosiaalisen median alustojen käyttöä osana manipulatiivisia disinformaatiokampanjoita. Nämä kampanjat käyttävät usein ihmisten ja bottien yhdistelmiä – automaatio-ohjelmistoja, jotka on rakennettu kopioimaan toimissaan aitoja käyttäjiä – saavuttaakseen tavoitteensa, siis vaikuttaakseen julkiseen elämään ja poliittisiin päätöksiin. Laskennallinen propaganda tutkimusalana pyrkii ymmärtämään tätä nousevaa digitaalisen disinformaation ja manipulaation ilmiötä.[2]

Terminä ja viestintämenetelmänä laskennallinen propaganda viittaa algoritmien, automaation ja ihmisohjauksen kautta toteutettuun harhaanjohtavan informaation tahalliseen levittämiseen digitaalisessa toimitilassa.[3] Laskennallinen propaganda siis muodostaa osan kyseenalaisista poliittisista menetelmistä kuten astroturffaus, valtiosponsoroitu trollaus ja uudet digitaalisen sodankäynnin muodot kuten Psyops tai

[1] Huom. Termi laskennallinen propaganda (tulee englanninkielisestä termistä 'Computational Propaganda') on kirjoittajan oma käännös termistä, jolle ei ole vakiintunutta suomenkielistä termiä tai määritelmää.

[2] Woolley, S. & Howard, P., 2019. Computational Propaganda Worldwide. Teoksessa Woolley, S. & Howard, P., *Computational propaganda: Political Parties, Politicians, and Political Manipulation on Social Media.* New York: Oxford University Press.

[3]. Woolley, S. & Howard, P. 2016. Automation, Algorithms, and Politics| Political Communication, Computational Propaganda, and Autonomous Agents—Introduction. *International Journal of Communication.* 10(0), 9.

InfoOps, jonka tarkoituksena on manipuloida verkossa olevaa informaatiota ihmisten mielipiteisiin ja käytökseen vaikuttamiseksi.[4]

Asiaa paremmin tuntevalle lukijalle tämä selitys voi riittää hyvin vastaukseksi kysymykseen. Mutta miten tämä kaikki todella tapahtuu? Miten laskennallinen propaganda mahdollistaa disinformaation leviämisen tai mielipiteiden manipulaation verkossa niin suurella skaalalla, että se voi vaikuttaa kokonaisen valtion poliittisiin prosesseihin? Miten nämä kampanjat toteutetaan ja miltä ne oikeasti näyttävät? Entä mitä näille asioille voidaan tehdä ja millaiset tekijät mahdollistavat niitä?

Laskennallinen propaganda ja laajamittaiset informaatio-operaatiot ovat todella nykypäivää. Vaikka sen lukeminen voi ajoittain tuntua vakoilunovellilta tai tiedefiktiolta, jokainen työssä esitellyistä keinoista perustuu todellisen maailman esimerkkeihin, tapauksiin ja tyypillisesti tutkimukseen. Informaatiosodankäynti valtioiden välillä on noussut uudelle tasolle, sekä Kiinan että Venäjän alkaessa toden teolla verrytellä informaatiolihaksiaan omien alueidensa ulkopuolella ja yhä useampien valtioiden laskiessa kyberjoukot omien kansalaistensa ’kimppuun’.

Samalla kuitenkin useimpien maiden lainsäädäntö raahaa surullisesti ilmiön perässä. Perinteiseen poliittiseen mainontaan pätevät säännöt eivät useimmissa tapauksissa yllä verkkoon ja esimerkiksi sosiaalinen media tarjoaa usein keinoja näiden säännösten kiertämiselle. Teknologian nopea kehitys tarjoaa erilaisia mahdollisuuksia teknologisesti luoville ratkaisuille, jotka voivat hyödyntää lainsäädäntöön jääneitä porsaanreikiä. Koska lainsäädäntöprosessit ovat usein hitaita ja monivuotisia, teknologisen kehityksen tapahtuessa joskus viikoissa tai kuukausissa, uusi lainsäädäntö saattaa jo valmistuessaan olla vanhentunut, puutteellinen tai kykenemätön vastaamaan uusimpiin haasteisiin ja ongelmiin.[5],[6]

Samanaikaisesti tutkimus kohtaa merkittäviä haasteita teknologiajättien läpinäkymättömän toiminnan ja kokonaisvaltaisen kivimuurittamisen seurauksena. Nämä

[4] Ibid.
[5] Fenwick, M., Kaal, W.& Vermeulen, E. 2017. Regulation Tomorrow: What Happens When Technology Is Faster than the Law? *American University Business Law Review*, Vol. 6. No. 3
[6] Malan, D. 2018. *The law can't keep up with new tech. Here's how to close the gap.* The World Economic Forum. Online. https://www.weforum.org/agenda/2018/06/law-too-slow-for-new-tech-how-keep-up/

toimet vaikeuttavat sekä lainsäädännöllisiä vastineita että tutkimusta, joka voisi valottaa parempaa kokonaisymmärrystä ilmiöstä ja ohjata vastatoimia disinformaatiota ja vaikutuskampanjoita vastaan. Samalla se tarjoaisi uusia keinoja asettaa vastuuta niille poliittisille toimijoille, jotka ovat päättäneet hyödyntää kyseenalaisempia keinoja kannatuksensa lisäämiseksi.

Yhtäaikaisesti itse sosiaalisen median alustat vastustavat voimakkaasti säätelyä, pääasiassa suojellakseen omaa tulostaan.[7] Ylivoimaisesti suurin osuus lähes kaikkien näiden yritysten, mutta erityisesti Googlen ja Facebookin tuotoista tulee mainosmyynnistä.[8] Vastauksena lainsäädännöllisille muutoksille ne ovatkin usein tarjonneet näennäistä läpinäkyvyyttä ja itseregulaatiota.[9] Usean vuoden jälkeen on kuitenkin alkanut näyttää yhä enemmän siltä, etteivät Facebookin itsesäätelyn toimet vastaa ongelmaan vaan pyrkivät lähinnä maskeeraamaan tai kiertämään sitä ja viivästyttämään sen kohtaamista.[10]

1.2. Työn tavoitteet

Viimeisten vuosien aikana olemme nähneet uudenlaisen disinformaatiouhan syntymisen, kasvun ja realisoitumisen. Laskennallinen propaganda on pysyvästi muuttanut sosiaalisen median luonteen ja vaatii meitä harkitsemaan omaa suhdettamme sosiaaliseen mediaan sekä uudelleenarvioimaan sen roolia yhteiskunnassamme. Siitä on tullut uhka sekä demokraattisen prosessin koskemattomuudelle mutta myös terveydellemme ja turvallisuudellemme. Sosiaalisen median kautta välittyvä disinformaatio ei ole vain uhka itsessään. Myöhemmin työssä näemme, miten se voi vaikuttaa globaalin kriisin aikana, syventäen jo olemassa olevia ongelmia sekä luoden uusia siellä, missä niitä ei ennen ollut. Mutta se voi myös luoda uusia haasteita sinne, missä niitä ei ennen ollut.

---

[7] https://www.nytimes.com/2019/03/30/technology/mark-zuckerberg-facebook-regulation-explained.html, https://www.itnews.com.au/news/google-warns-aussie-users-against-proposed-media-code-551806, https://www.wired.com/story/opinion-oh-sure-big-tech-wants-regulationon-its-own-terms/

[8] Facebook. 2018. *Annual Report*. https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2018-Annual-Report.pdf., https://www.forbes.com/sites/greatspeculations/2019/12/24/is-google-advertising-revenue-70-80-or-90-of-alphabets-total-revenue/#10e250f94a01

[9] Mortensen, J. 2019. *Status update: Facebook's self-regulation trumps transparency.* Asia & The Pacific Policy Society Policy Forum.

[10] https://www.theguardian.com/commentisfree/2019/oct/31/mark-zuckerberg-facebook-regulate

Viime vuosina nähty median kahtiajako ja yhteiskunnan polarisoituminen Yhdysvalloissa on saanut kannattimia yhdysvaltalaista yhteiskuntaa vastaan kohdistetuista Venäjän laajamittaisista manipulatiivisista vaikutus- ja disinformaatiokampanjoista. Koronaviruksen aikana yhteiskuntiamme kohdanneet kriisit eivät ole vain pahentuneet vaan saaneet uusia ulottuvuuksia, disinformaation ollessa ennennäkemättömän laajalle levinnyttä ja samalla tehokasta. Tämä on johtanut heikentyneeseen yhteiskunnalliseen luottamukseen, hoito- ja turvaohjeiden ohittamiseen sekä terveydelle ja hengelle vaarallisiin hoitoratkaisuihin kuten käsidesin juomiseen parannuskeinona virukseen.

Keskeinen ongelma on äärimmäisen laajalle levinnyt disinformaatioilmasto sekä eri toimijoiden keskenään kilpailevat intressit. Tavalliselle tarkastelijalle kokonaisvaltainen ymmärryksen muodostaminen aiheesta ei ole vain haastavaa vaan lähes mahdotonta. Sekä sosiaalisen median alustojen että itse disinformaatiota levittävien toimijoiden etuna on se, että ongelma säilyy vaikeaselkoisena, teknisenä ja tavalliselle seuraajalle usein liian vaikeana ymmärtää. Ongelman teknisyys on myös ollut etu, jota sosiaalisen median alustat itse ovat hyödyntäneet kohdatessaan kysymyksiä ja kritiikkiä niin lainsäätäjiltä, asiantuntijoilta, kuin myös julkisen mielipiteen taholta.

Tämä työ tarkastelee ilmiötä luomalla katsauksen käynnissä olevaan disinformaatiokriisiin sekä ilmiöihin sen taustalla ja pyrkii samalla häivyttämään siihen liitetyn epäselvyyden ja tarpeettoman monimutkaisuuden. Mitkä mekanismit mahdollistavat disinformaation ennennäkemättömän laajan levinneisyyden sekä tehokkuuden? Millä keinoilla pahantahtoiset toimijat levittävät viestejään sosiaalisessa mediassa? Mistä nämä viestit tulevat tai lähtevät? Mitä sosiaalisen median alustat ovat tehneet asialle? Entä kenelle vastuu ilmiöstä todella kuuluu. Mitä sille pitäisi tehdä?

Työn tavoite on myös vastata kysymyksiin tavalla, joka on ymmärrettävä myös sellaiselle lukijalle, joka ei aiemmin ole perehtynyt aiheeseen. Sen tarkoitus on tehdä selkeäksi se, että pohjimmiltaan kyseessä ei ole teknologinen vaan säätelyllinen ongelma. Vaikka ilmiö tapahtuu virtuaalisessa ympäristössä, sen seuraukset näkyvät jokapäiväisessä maailmassamme eivätkä myöskään ratkaisut siihen loppujen lopuksi ole vain teknisiä vaan usein lainsäädännöllisiä, eettisiä ja inhimillisiä. Haasteet, joita meidän yhteiskuntana tulee kohdata ratkaistaksemme ongelma eivät liity algoritmeihin vaan vastuuseen. Lopulliset ratkaisut ongelmaan eivät ole teknisiä vaan lainsäädännöllisiä.

Työ on kirjoitettu hyvin vahvasti kartoittavana. Tätä ratkaisua tukee sekä (a) miten vähän ilmiöstä on kirjoitettu (”laskennallista propagandaa jollain tavalla käsitteleviä töitä Suomen kielellä on kirjoitettu 2 kappaletta”) sekä (b) miten huonosti ilmiö on yleisesti ymmärretty. Sekä perinteinen ymmärrys ilmiöstä (niin kutsuttu intuitiivinen, esimerkiksi lainsäätäjien tai aiheeseen ei-perehtyneiden tutkijoiden käsitys) kuin myös ilmiöstä populaarikulttuurissa (media, elokuvat, televisio, internet ja sosiaalinen media) vallitseva ymmärrys ovat usein sisäisesti ristiriitaisia, eivätkä vain väärässä vaan ilmiöstä ja ongelmista myös täydellisen tietämättömiä.[11]

Tässä suhteessa riippumatta työn vahvasti kartoittamasta luonteesta, se palvelee tärkeää ja uraauurtavaa tehtävää: Se on ensimmäinen näitä keinoja ja ilmiötä laajasti käsittelevä suomenkielinen työ. Samalla se pyrkii valottamaan ymmärrystä ilmiöstä, korjaamaan siihen liittyviä puutteita sekä nostamaan tietoisuutta äärimmäisen tärkeästä ja kriittisestä ongelmasta.

1.2. Työn rakenne

Luku 1 on johdantoluku perustellen motivaation ilmiön tutkimiseen, työn käsittelemät keskeiset ongelmat ja tavoitteet sekä kuvaten työn rakenteen. Luku 2 siirtyy yleiseen toimijoiden ja alustojen kuvaukseen muodostaen yleiskatsauksen ilmiöön ja sitä ympäröiviin tekijöihin. Luku 3 keskittyy tapauskuvaukseen, jossa käsitellään kahta viimeisen vuosikymmenen merkittävintä disinformaatiotapausta. Tapaukset on valittu niiden laajan kattavuuden, tunnettavuuden sekä niiden aikaansaaman vaikutuksen takia. Ne edustavat uhkaa yhteiskuntiemme demokratialle ja demokraattisen prosessin koskemattomuudelle, turvallisuudellemme ja terveydellemme sekä kyvyllemme selviytyä kriisistä. Ne myös antavat lukijalle kuvauksen laskennallisen propagandan todellisen maailman vaikutuksista. Näiden tapausten tarkoitus on myös havainnollistaa lukijalle aiheen tärkeyttä, vakavuutta ja ajankohtaisuutta sekä perustella, miksi ilmiön ymmärtäminen ja jatkotutkimus olisi äärimmäisen tärkeää.

Löydetyistä suomen kielellä kirjoitetuista töistä laskennallista propagandaa käsittelevät Dookie Gyan vuoden 2019 mediatutkimus-aiheinen Pro Gradu *Julkison mahdollisuus algoritmien ja alustojen aikakaudella: teoreettinen dystopia* sekä Mikko Hämäläisen vuoden 2020 yleisen valtio-opin Pro Gradu *Propagandaa kyberavaruudessa: Venäjän trollitehtaan toiminta sosiaalisessa mediassa*.

Ensimmäinen luvun kolme käsittelemä tapaus, Venäjän vaalivaikutus Yhdysvaltain 2016 vaaleissa, kuvaa disinformaation laajamittaista käyttöä kansakunnan julkisen mielipiteen manipuloimiseksi maailman varakkaimmassa ja voimakkaimmassa maassa. Se on esimerkki hienostuneen toimijan vaalivaikutuksesta yli 300 miljoonan kansalaisen yhteiskunnassa ja kuvaa, miltä tällainen operaatio voi näyttää. Toinen tapauksista käsittelee vuoden 2020 koronavirus-pandemian yhteydessä levitettävää disinformaatiota. Tapaus toimii kuvauksena disinformaation levityksestä globaalin kriisin keskellä ja havainnollistaa myös sen tehokkuutta, levinneisyyttä ja vaikutuksia. Luku kolme sisältää myös viitteitä lukuun neljä, joka sisältää tarkempia kuvauksia luvussa kolme mainituista keinoista ja voi auttaa lukijoita paremmin ymmärtämään näitä keinoja sekä niiden toimintaa.

Luku 4 on työn teknisin osuus ja käsittelee laskennallisen propagandan keinoja ja termistöä. Se tekee syväsukelluksen laskennallisen propagandan keinoihin, jotka mahdollistavat luvussa kaksi ja kolme nähdyt esimerkit, sekä esittelee myös joitakin uusia, näissä luvuissa vielä käsittelemättömiä keinoja, joita todellisen maailman toimijat kuitenkin jo soveltavat. Jokaiseen keinoon liitetään lyhyt, todellisen maailman esimerkki sen käytöstä keinon havainnollistamiseksi lukijalle. Luvun tarkoitus on auttaa lukijaa ymmärtämään eri keinojen merkitykset ja tavoitteet sekä tarjota teknisen tason ymmärrys siitä, miten laskennallisen propaganda mahdollistaa disinformaation leviämisen. Se myös täydentää lukua kolme, kuvaamalla useita luvussa mainituista keinoista yksityiskohtaisemmin ja tarkemmin. Yhdessä luvut kaksi, kolme ja neljä muodostavat vastaukset kysymyksiin kuka, mitä ja miten.

Luku 5, johtopäätökset ja toimenpide-ehdotukset, siirtyy johtopäätöksiin työstä ja kokonaisuudesta. Luku 5.1 esittelee kolme laajaa, normatiivisia toimenpide-ehdotusta, jotka on muodostettu vastaamaan työn esittämiin keskeisiin ongelmiin. Nämä toimenpiteet alleviivaavat askelia, joita yhteiskuntien, tutkijoiden ja ylikansallisten toimijoiden tulisi ottaa yhdessä vastatakseen ilmiöön ja muodostaakseen koherentin vastuksen meitä uhkaavalle haasteelle.

Työ käyttää alaviitejärjestelmää, joka sisältää kokonaiset lähdeviitteet osana alaviitteitä. Tämän takia työ ei sisällä lähdeluetteloa. Aineistokuvaus on kuitenkin sisällytetty Liitteeseen 1, joka on löydettävissä työn lopusta.

2. Toimijat ja alustat

Disinformaatio ja laskennallinen propaganda eivät rajoitu yksinään tietyille alustoille tai sivuille. Kekseliäät valtiolliset tai kaupalliset toimijat käyttävät laajaa keinovalikoimaa paikallisista foorumeista globaaleihin sosiaalisen median alustoihin.[12] Toimijat kattavat valtioita, poliittisia puolueita, konsultointiyrityksiä, kansalaisaktivisteja ja harrastelijoita.

Laskennallisen propagandan rooli työn kontekstissa on tyypillisesti mahdollistaa informaation tehokasta levittämistä. Laskennallinen propaganda ei ole päämäärä itsessään, (lukuun ottamatta kenties kompetenssien rakentamista tällä osa-alueella) vaan keino toimijan laajemman tavoitteen saavuttamiseksi. Sen ei tarvitse olla pahantahtoista tai manipulatiivista. Tästä hyvänä esimerkkinä ovat esimerkiksi Kanadassa käytetyt aktivistien rakentavat läpinäkyvyysbotit, jotka twiittaavat nimettöminä tehdyistä Wikipedia-muutoksista, jotka tulevat valtion IP-osoitteista, tai *Project Arachnidin* käyttämä yksinkertaisempi palvelijabotti, joka automaattisesti tunnistaa ja merkitsee pornografista materiaalia, jossa on mukana alaikäisiä sekä kirjaa automaattisen ilmoituksen laittomasta sisällöstä.[13]

Valitettavasti suurin osa käytetystä laskennallisesta propagandasta ei kuitenkaan palvele julkista hyvää tai yhteisön etuja. Viimeisten vuosien aikana julkisuuteen on noussut toistuvasti uusia tapauksia laskennallisen propagandan käytöstä poliittisessa manipulaatiossa, vaalisekaantumisessa, disinformaation levittämisessä, joidenkin ryhmien äänen suppressoinnissaja toisten amplifikaatiossa.(Katso luvut 4.2 ja 4.3) Botit ja bottiverkot, amplifikaatio ja astroturffaus ovat johtaneet senaatin tutkintaan Yhdysvalloissa, syviin epäilyksiin vaalisekaantumisesta Brexit-äänestyksestä Iso-Britanniassa sekä EU:n kannanottoihin Kiinaa ja Venäjää vastaan Euroopassa.[14] (Katso myös luvut 4.1 ja 4.5)

---

[12] Volcheck, D. 2015. *One Professional Russian Troll Tells All.* Radio Free Europe. https://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html

[13] McKelvey, F. & Dubois, E. *Computational Propaganda in Canada: The Use of Political Bots.* Computational Propaganda Research Project, Working Paper No. 2017.6

[14] Mm. European Parliament. 2019. *EU prepares itself to fight back against hostile propaganda.* Press Release., United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views.* Report of the Select Committee on Intelligence. 116th Congress, 1st. session., https://www.theguardian.com/world/2020/jun/10/eu-says-china-behind-huge-wave-covid-19-disinformation-campaign., https://www.politico.eu/article/russia-china-disinformation-coronavirus-covid19-facebook-google/., https://www.bbc.com/news/uk-politics-53480682.

Kuten laskennallinen propaganda ei rajoitu sisällössään tietyille sivuille tai alustoille, myöskään sitä soveltavia toimijoita ei voida rajata pelkästään tämän työn puitteissa käsiteltyihin. Vaikka työn pääpaino on tapauskuvauksen kautta vahvasti valtiollisissa toimijoissa, myös kaupalliset toimijat ja poliittiset puolueet osallistuvat kasvavalla innolla laskennallisen propagandan soveltamiseen omien tavoitteidensa saavuttamiseksi. Konsultointi-yritykset myyvät ”räätälöityjä vaikutuskampanjoita sinun viestisi levittämiseksi” tarjoten palveluita erilaisten työkalujen, välineiden ja ohjelmistojen myynnistä ja koulutuksesta botteihin, valekäyttäjiin, bottiverkkoihin tai kokonaisiin sosiaalisen median manipulaatiokampanjoihin. Asiakkaat voivat olla yrityksiä, jotka haluavat puskea läpi tiettyä viestiä tai haluavat parantaa kykyjään seuraavan PR-kriisin käsittelemiseksi, poliittisia kampanjoita, jotka haluavat etulyöntiaseman kilpakumppaneihinsa tai valtioita, jotka tarvitsevat kompetensseja tai etäisyyttä ja ”uskottavan tietämättömyyden”[15] toimilleen.[16]

Samalla teknologian kehitys tuo uusia mahdollisuuksia laskennallisen propagandan levittämiselle kuten myös haasteita yrityksille ja toimijoille. Sosiaalisen median alustojen sekä tutkijoiden (joiden yhteistyö alustojen kanssa on merkittävän rajattua, johtuen itse alustojen vastahakoisuudesta osallistua yhteistyöhön[17]) haasteena on jatkuvasti parantaa algoritmejaan bottien ja koordinoidun epäautenttisen käytöksen havaitsemiseksi. Toisaalta tämä ajaa palveluita tarjoavia toimijoita kehittämään ohjelmistojaan, algoritmejaan ja toimitapojaan vaikeammin havaittaviksi. Samalla siis kirjo on hyvin laaja. Useimmat botit ovat osa todella yksinkertaisia amplifikaatioverkostoja (termien tarkempi määrittely sekä keinojen kuvaus luvussa 3), omaten mitä pinnallisimman ja helposti tunnistettavan profiilin sekä esittäen käytökseltään todella helposti havaittavia toistuvuuksia, säännönmukaisuuksia sekä tunnuspiirteitä. Toisaalta kehittyneemmät ja paremmin resursoidut toimijat kehittävät syvemmälle istutettuja, aidompia ja monimutkaisempia botteja tai hybridibotteja, joiden tunnistaminen laajamittaisesti vaatii sekä algoritmeilta että tutkijoilta yhä suurempia ponnistuksia.

---

[15] (“Plausible Deniability”.)
[16]Singularex. 2018. *The Black Market for Social Media Manipulation.* NATO Stratcom COE.
[17]Hyvänä esimerkkinä alustojen vastahakoisuudesta osallistua dialogiin sekä jakaa resurssejaan tutkijoiden kanssa on Venäjän sekaantuminen Yhdysvaltain 2016 vaaleihin, joissa esimerkiksi Facebookin ja erityisesti Googlen jakamissa tietokannoissa oli hyvin keskeisiä puutteita ja vajavaisuuksia. Lähde: Howard, P., Ganesh, B., Dimitra, L., Kelly, J.& Francois, C., 2018. *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* Computational Propaganda Research Project.

Tämän lisäksi poikkeuksellisen haastavaa ilmiön havainnoinnista tekee se, että keskeisin tapa kerätä ilmiöstä tietoa on pyrkiä havainnoimaan siihen osallistuvien toimijoiden käytöstä sosiaalisessa mediassa. Keskeinen ongelma tämän kanssa kuitenkin on, että nämä toimijat pyrkivät välttämään havaituksi tulemista. Tämä tarkoittaa, että sekä alustat ja tutkijat tunnistavat merkittävästi todennäköisemmin niitä toimijoita, jotka ovat vähemmän kehittyneitä, teknologisesti vanhentuneita tai omaavat heikommat kompetenssit. Tämä johtaa kuitenkin keskeiseen haasteeseen siinä, että se saattaa joissakin tapauksissa tuottaa havainnointiharhan, jossa alustat ja tutkijat löytävät merkittävästi enemmän yksinkertaisia ja vähemmän kehittyneitä toimijoita mutta eivät välttämättä tunnista hienostuneimpia toimijoita jotka onnistuvat välttämään havaitsemista. Tämä voi johtaa vinoutuneeseen kuvaan toimijoista sekä toimijoiden toimikyvyistä. Samalla tämänkaltaisen havaintoharhan merkittävyyttä, laajuutta tai realistisuutta on vaikea arvioida. Samalla sen mahdollinen olemassaolo olisi kuitenkin hyvä tiedostaa ja huomioida alan kirjallisuudessa ja tutkimuksessa.

Keskusteltaessa erilaisista toimijoista, alustoista ja kampanjoista, on tärkeää tiedostaa, että ilmiön havainnointi on osittain pintapuolista. Johtuen massiivisesta määrästä päivittäin tuotettua sisältöä suuri osa disinformaatiosta jää todennäköisesti havaitsematta täysin (Facebook itse arvioi, että noin 5 % sen käyttäjistä, eli noin 120 miljoonaa, eivät ole aitoja käyttäjiä.) Vaikka Facebook ei jaa päivittäisten päivitysten määrää, noin 350 miljoonaa valokuvaa lisätään alustalle päivittäin ja sivuston mukaan sillä on noin 2.5 miljardia aktiivista kuukausittaista käyttäjää. Se tuottaa päivittäin noin 4 petabyteä dataa.[18] Johtuen sekä tuotetun informaation määrästä sekä siitä, että sosiaalisen median alustat ovat tyypillisesti hyvin vastahakoisia antamaan tutkijoille pääsyä alustojensa tuottamaan dataan, suurin osa tutkimuksesta sosiaalisessa mediassa tapahtuviin disinformaatio- tai manipulaatiokampanjoihin perustuu kohtalaisen pieniin otoksiin. Näiden otosten merkityksellisyyttä ei ole laajasti arvioitu. Ne voivat kuitenkin olla

[18] Suhteutettuna, valokuvan koko voi olla noin 10 megabyteä, ja 2 tunnin elokuvan koko noin 4 megabyteä. Tavallisen graduatyö on kooltaan noin 0.5-1 megabyteä. Tyypillisessä uudessa työläppärissä voi olla noin 500-1000 gigabyteä tallennustilaa. 1 gigabyte on 1000 megabyteä. 1 terabyte on 1000 gigabyteä. 1 petabyte on 1000 terabyteä. 1 petabyte vastaa siis noin 1000 – 2000 tuhannen tavallisen kannettavan tietokoneen tallennustilaa, tai noin 2 miljardia gradutyötä.
Lähteet: https://www.brandwatch.com/blog/facebook-statistics/., https://www.omnicoreagency.com/facebook-statistics/., https://www.huffpost.com/entry/facebook-fake-accounts_n_5ce6d266e4b0cce67c872727

ongelmallisia johtuen erityisesti sosiaalisen median taipumuksesta voimakkaaseen klusterointiin sekä ryhmäytymiseen, jolloin edustavan otoksen saaminen on haastavampaa ja vaatii yleisesti eriytetympiä menetelmiä.[19]

Työn luku 2.1 siirtyy käsittelemään valtiollisia toimijoita ja kyberjoukkoja. Tämän työn kontekstissa kyberjoukoilla viitataan terminä järjestyneisiin toimijoihin, joiden pyrkimyksenä on julkisen mielipiteen systemaattinen manipulointi verkossa. Luvussa 2.1 kyberjoukkoina voivat olla valtion alaisuudessa, ohjauksessa tai sopimuksella sen kautta operoivia toimijoita. Näitä voivat olla joko valtion virastot, instituutit tai muut yksiköt, armeijan omat erikoisyksiköt kuten Britannian Armeijan 6 Divisioona tai viestintätoimistot, jotka myyvät palveluitaan valtiolle sopimuksen alaisuudessa.[20]

Tästä määritelmästä erotetaan kuitenkin sellaiset ei-valtiolliset toimijat, jotka tyypillisesti osallistuvat tämänkaltaiseen toimintaan demokraattisissa maissa. Esimerkkeinä tästä ovat poliittiset puolueet, etujärjestöt ja muut poliittiset toimijat, jotka käsitellään luvussa 2.2.

Luku 2.3 käsittelee omana osionaan kaupalliset toimijat kuten poliittisen viestinnän- ja konsultoinnin palveluita tarjoavat yritykset.

2.1. Valtiolliset toimijat ja kyberjoukot

Oxfordin Internet Research Institutin alaisena toimiva Computational Propaganda Research Project on määritellyt kyberjoukot tarkoittamaan valtion, armeijan tai poliittisen puolueen joukkoja, jotka työskentelevät julkisen mielipiteen manipuloimiseksi sosiaalisessa mediassa.[21] Tämän työn määritelmä on hieman laajempi, sillä se sisältää myös sellaiset yksiköt, jotka pyrkivät torjumaan näitä hyökkäyksiä sekä kehittämään tehokkaaseen torjumiseen tarvittavia valmiuksia.

[19]A. Alsayat & H. El-Sayed. 2016. *Social media analysis using optimized K-Means clustering*. IEEE 14th International Conference on Software Engineering Research, Management and Applications (SERA)

[20] Bradshaw, S. & Howard, P. 2017. *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. Computational Propaganda Research Project.* Working paper no. 2017.12., https://www.telegraph.co.uk/news/2019/07/31/british-army-engage-social-media-warfare-senior-soldier-announces/.

[21] Bradshaw, S. & Howard, P. 2017. *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation.* Computational Propaganda Research Project. Working paper no. 2017.12.

Kyberjoukot ovat tyypillisesti joko valtiollisen toimijan alaisuudessa tai ohjauksessa toimivia osapuolia, sen kontraktoimia pysyviä toimijoita tai erillisiä kaupallisia toimijoita, jotka myyvät palveluitaan ja osaamistaan valtiolle. Näitä voivat olla joko valtion virastot, instituutit tai muut yksiköt, armeijan erityisjoukot tai -osastot, valtionjohdon omistamat tai läheisesti tukemat yritykset tai tutkimusyksiköt tai itsenäiset viestintätoimistot.[22] Tämä määritelmä ei kuitenkaan sisällytä poliittisia puolueita, jotka käsitellään omana osionaan luvussa 2.2.

Kyberjoukkojen tavoitteet tässä kategoriassa voidaan laajasti jakaa kahteen ryhmään: Informaatiovaikuttamista toteuttavat ja siltä puolustautuvat. Erityisesti länsimaisissa demokratioissa kyberjoukot keskittyvät tyypillisesti enemmän hyökkäysten torjuntaan ja vapaan puheen puolustamiseen. Toisaalta taas autoritaarisemmissa hallinnoissa kyberjoukot keskittyvät tyypillisesti informaatiovaikuttamiseen ja järjestäytyneeseen sosiaalisen median manipulaatioon kotimaassa. Sen lisäksi ne saattavat joissakin tapauksissa pyrkiä toteuttamaan informaatio-operaatioita sekä järjestäytyneitä sosiaalisen median manipulaatiokampanjoita ulkomailla, jolloin ne pyrkivät usein joko disinformaation levittämiseen tai muihin strategisen viestinnän ja manipulaation muotoihin tavoitteidensa saavuttamiseksi.[23]

Toistaiseksi eri maiden tarkoista kapasiteeteista, organisaatiorakenteista sekä toimijoista tiedetään kohtalaisen vähän. Seitsemän valtion tiedetään käyttävän erilaisia sosiaalisen median alustoja, pääasiassa Facebookia ja Twitteriä, osana ulkomaisia vaikutusoperaatioita. Tunnistetut valtiot ovat Kiina, Venäjä, Intia, Iran, Pakistan, Saudi Arabia ja Venezuela.[24] Toisaalta esimerkiksi vain Kiinan ja Venäjän rooli erityisesti länsimaisessa kontekstissa on ollut poikkeuksellisen korostunut viimeisten vuosien aikana, mahdollisesti osoittaen näiden toimijoiden pyrkivän ajamaan tavoitteitaan aggressiivisemmin tai vain omaavan merkittävästi suuremmat resurssit.

Toimijoista on kuitenkin opittu jonkin verran viime vuosina. Vuonna 2019 Ison-Britannian Armeija järjesti uudelleen 6 divisioonansa vastaamaan erityisesti

[22] Ibid.
[23] Ibid.
[24] Bradshaw, S. & Howard, P. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation.* Computational Propaganda Research Project.

teknologisesti edistyneiden toimijoiden (esimerkiksi Venäjän) esittämiin uhkiin sekä kehittämään sen kapasiteetteja asymmetrisen sodankäynnin osa-alueella.[25]

Venäjän kohdalla merkittävä osa sen disinformaatioon, informaatiosodankäynnin ja sosiaalisen median manipulointiin tähtäävistä operaatioista on tunnistettu osaksi Pietarissa toimivaa Internet Research Agencya, tai IRA:ta.[26] Tämän lisäksi Venäjän tiedustelupalvelun GRUn on huomattu suorittavan kybersodankäynnin hyökkäyksiä muiden operaatioiden tukena tai niiden rinnalla. Se on tunnistettu päätoimijaksi ainakin Yhdysvaltoihin 2016 kohdistuneissa hyökkäyksissä äänestysinfrastruktuuria ja elektronisia äänestysjärjestelmiä vastaan. Tämän lisäksi se oli vastuussa onnistuneesta kyberhyökkäyksestä silloista presidenttiehdokas Hillary Clintonia ja DNC:tä[27] kohtaan, joka johti tietovarkauteen sekä Clintonin sähköpostien vuotamiseen ennen 2016 presidentinvaaleja.[28] (Luvut 4.7 ja 4.8 sisältävät kuvauksen DDoS-hyökkäyksistä ja Doksauksesta liittyen sekä DNC:n hyökkäykseen että äänestysinfrastruktuuriin kohdistettuihin iskuihin).

Kiinan tapauksessa sen organisaatiorakenteesta, toimijoista tai kapasiteeteista tiedetään hyvin vähän. Kiina operoi kuitenkin mahdollisesti suurinta ja parhaiten rahoitettua koneistoa sen työllistäessä arvioilta noin 300 000–2 000 000 työntekijää kotimaisten ja ulkomaisten operaatioidensa yhteydessä.[29]

Sosiaalisen median järjestäytynyt manipulaatio on yleisesti hyvin laajalle levinnyttä. Vuoden 2019 tutkimus arvioi, että todisteita järjestäytyneistä manipulaatiokampanjoista löytyi 70 maasta. Tutkimus myös arvioi, että 26 maassa laskennallista propagandaa käytetään informaatiohallinnan keinona, jossa se on työkalu esimerkiksi ihmisoikeuksien

---

[25] http://www.warfare.today/2019/08/01/british-army-launches-new-6th-division/

[26] Special Counsel Robert S. Mueller. 2019. *Report on The Investigation Into Russian Interference in the 2016 Presidential Election. Volume I of II*. U.S. Department of Justice., United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views*. Report of the Select Committee on Intelligence. 116th Congress, 1st. session.

[27] (DNC, Democratic National Committee. Yhdysvaltojen demokraattisen puolueen keskusjärjestö.)

[28] United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts Against Election Infrastructure with Additional Views*. Report of the Select Committee on Intelligence. 116th Congress, 1st. session.

[29] Bradshaw, S. & Howard, P. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Computational Propaganda Research Project.

toteutumisen estämiselle, poliittisten kilpakumppanien viestien ja toiminnan alleviivaukselle sekä eriävien mielipiteiden vaimentamiselle. Seitsemän valtion kohdalla tiedetään myös näiden valtioiden käyttävän sosiaalista mediaa vaikutusoperaatioihin ulkomailla.[30]

Valtiollisten toimijoiden rooli ajamassa laskennallisen propagandan ja disinformaation leviämistä sosiaalisessa mediassa ei ole epätyypillinen. Sekä Venäjällä että Kiinalla on pitkä historia propagandan sekä disinformaation levittämisestä sekä omien kansalaistensa että lähinaapureidensa joukossa. Näin nämä toimijat ovat omanneet erinomaiset mahdollisuudet siirtää jo valmiiksi olemassa olevat kompetenssinsa sosiaalisen median toimintaympäristöön, joka on pitkälti toiminut jatkeena jo olemassa olevalle disinformaatio- ja propagandakoneistolle. Se on myös mahdollistanut entistä tehokkaamman kohdennuksen ja amplifikaation tämän koneiston viesteille.[31] Sekä Venäjän että Kiinan suoraan omistama tai läheisesti tukema valtiollinen media on toiminut tehokkaana disinformaation levittäjänä muun muassa 2020 koronavirus-pandemian yhteydessä, tavoittaen mahdollisesti jopa satoja miljoonia ihmisiä sosiaalisen median avustamana.[32]

Toisena selittävänä tekijänä valtiollisten toimijoiden merkittävälle roolille ilmiössä on myös sen yleinen haastavuus ja vaaditut resurssit. Vaikka yksityisillä kaupallisilla toimijoilla on yhtäaikaisesti erinomaiset mahdollisuudet rakentaa kompetensseja ja osallistua toimintaan, tietyt piirteet tekevät valtiolliset toimijat paremmin sopiviksi pitkäaikaisiin projekteihin ja kompetenssien rakentamiseen: vaadittu organisaation taso, merkittävät resurssit ja vaatimus pitkäjänteiseen toimintaan sekä monivuotisiin projekteihin merkitsevät, että valtiolliset organisaatiot ovat toimijoina luonnollisesti keskeinen osa ilmiötä.

---

[30] Ibid.

[31] Sanovich, S., Origins of Misinformation. Teoksessa Woolley, S. & Howard, P. 2019. *Computational propaganda: Political Parties, Politicians, and Political Manipulation on Social Media.* New York: Oxford University Press.

[32] Rebello, K., Schwieter, C., Schliebs, M., Joynes-Burgess, K., Elswah, M., Bright, J. & Howard, P. 2020. *Covid-19 News and Information from State-Backed Outlets Targeting French, German and Spanish-Speaking Social Media Users*. COMPROP Data Memo 2020.4., Bright, J., Au, H., Bailey, H., Elswah, M., Schliebs, M., Marchal, N., Schwieter, C., Rebello, K., Howard, P.*, Coronavirus Coverage by State-Backed English-Language News Sources.* COMPROP Data Memo 2020.2

2.2. Poliittiset toimijat

Toinen merkittävä toimijaryhmä on ollut ja tulee olemaan poliittisten toimijoiden ryhmä. Vaikka poliittisten toimijoiden rooli Venäjän ja Kiinan kaltaisissa autoritaarisissa maissa ei ole juurikaan läsnä, ne edustavat kuitenkin merkittävää toimijaryhmää monissa demokraattisissa monipuoluejärjestelmissä.

Poliittiset puolueet sekä laajemmin poliittiset toimijat kuten etujärjestöt tai kampanjat, käyttävät laskennallista propagandaa tyypillisesti oman etunsa tai asiakysymystensä ajamiseen kotimaassa. Tällöin ne voivat esimerkiksi haluta pyrkiä saamaan etulyöntiaseman poliittisiin kilpakumppaneihinsa.

Poliittisten puolueiden kampanjoiden kohdalla kampanjat harvoin ovat itse vastuussa sosiaalisen median vaikutuskampanjoiden toteutuksesta. Ne ostavat usein teknistä osaamista yksityisiltä yrityksiltä, joilla on parempi hallinta laskennallisen propagandan keinoista. Näitä ovat esimerkiksi viestintä- ja poliittisen konsultoinnin yritykset. Tämä muodostaa myös merkittävän osan ekosysteemiä yksityisen puolen toimijoille, joita tarkastellaan lyhyesti luvussa 2.3. Tässä luvussa määritellyn poliittisten toimijoiden ja yksityisen sektorin yhteistyöstä löytyy lisää esimerkkejä luvusta 3, laskennallinen propaganda.

Poliittisten toimijoiden ja yksityissektorin toimijoiden yhteistyöstä on kuitenkin merkittäviä etuja. Ilmiselvien tehokkuus- ja kompetenssihyötyjen lisäksi toisena etuna on ainakin jossakin määrin etäisyyden luominen itse kampanjaan sekä tietynasteisen suojan antaminen poliittiselle toimijalle verrattuna siihen, että se itse käyttäisi näitä kyseenalaisia keinoja osana kampanjaansa. Yksityinen sektori tarjoaa merkittäviä innovaatioita sekä on huomattavan notkea toiminnassaan, mikä sopii hyvin teknologisen kehityksen kärkeen pyrkivälle poliittiselle kampanjalle. Sopimuksen kautta kontraktointi ja palveluiden osto antavat sen testata nopeasti erilaisia menetelmiä, seurata ja tarkkailla niiden toimivuutta ja tarvittaessa luopua joistain tai lisätä niiden käyttöä. Tämä sopii erityisen hyvin nopeasti muuttuvaan ja kehittyvään toimialaan, jossa keinot vaihtuvat jatkuvasti ja innovaation sekä muutoksen taso on poikkeuksellisen korkea. Onkin todennäköistä, että yksityisten ja poliittisten toimijoiden yhteistyö tällä alalla tulee jatkossakin pysymään yleisenä. On itseasiassa todennäköistä, että tämän yhteistyön suosio tulee vain kasvamaan tulevaisuudessa.

Niin sanotuissa länsimaisissa, ’vapaissa’ demokratioissa on nähty vähemmän tapauksia, joissa puolueet käyttäisivät botteja, algoritmista manipulaatiota, astroturffausta tai valekäyttäjiä kampanjoidensa tukena.[33] Vaikka näitä tapauksia on olemassa, ne eivät ole vielä merkittävän laajalle levinneitä useimmissa maissa. Tähän voi vaikuttaa menettelyn tuoma negatiivisen julkisuuden mahdollisuus tai äänestäjien potentiaalinen vastareaktio. Puolueen jäädessä kiinni avoimesta yrityksestä manipuloida äänestäjiä. julkista mielipidettä tai prosessia, vihainen reaktio sekä äänestäjiltä että julkisuudelta voisi olla merkittävän todennäköinen.

Toisaalta merkittävänä kontrastina ovat kehittyvät maat sekä eteläinen pallonpuolisko, jossa poliittiset toimijat ovat olleet nopeita omaksumaan sosiaalisen median mukanaan tuomia mahdollisuuksia, huolestumatta liikaa niiden tuomista moraalisista tai eettisistä ongelmista.[34] Latinalaisessa Amerikassa Brasilia on ollut nopea omaksumaan käyttöönsä koko laskennallisen propagandan kirjon. Siellä sosiaalisen median kautta toimivat botit, valekäyttäjät ja amplifikaatio muodostavat merkittävän osan puolueiden välisestä poliittisesta kilpailusta. Brasiliassa laskennallisen propagandan arvioidaan olleen merkittävä selittävä tekijä muun muassa 2014 presidentinvaaleissa, 2015–2016 presidentin virkarikosprosessissa ja 2016 Rio De Janeiron kunnallisvaaleissa. Muun muassa organisoitu bottitoiminta sekä amplifikaatio ja massaviestintä Whatsappin kautta näyttelivät merkittävää roolia osana kaikkia näitä tapahtumia.[35]

Brasilian tapauksessa voidaan huomioida myös maan paikalliset vaalilait, jotka estävät puolueita maksamasta vaalimateriaalin levittämisestä sosiaalisessa mediassa aktiivisten vaalien aikana. Laki on kuitenkin muotoiltu niin, ettei se kiellä yksityisiä toimijoita tekemästä näin poliittisten kampanjoiden puolesta, mikäli ne eivät ole suoraan kytköksissä näihin kampanjoihin. Lakia onkin kritisoitu vanhentuneeksi ja riittämättömäksi rikkomusten valvontaan. Brasilian tapauksessa on tullut hyvin nopeasti

[33] Woolley, S. & Howard, P. 2019. Computational Propaganda Worldwide. Teoksessa Woolley, S. & Howard, P. *Computational propaganda: Political Parties, Politicians, and Political Manipulation on Social Media.* New York: Oxford University Press.
[34] Arnaudo, D. 2019. Political Bot Intervention During Pivotal Events. Teoksessa Woolley, S. & Howard, P. *Computational propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. New York: Oxford University Press.
[35] Ibid.

selväksi, että laki ei huomioi riittävästi nykyistä teknologisen kehityksen tasoa ja on siitä syystä yksityisiin toimijoihin kohdistuvien rajaustensa takia riittämätön todellisen maailman olosuhteisiin.[36]

Läntisessä maailmassa Donald Trumpin kampanjaa, Brexit-kampanjaa, Puolan PiS-puoluetta ja Saksan AfD:tä vastaan on esitetty hyvin perusteltuja ja tarkasti dokumentoituja syytteitä laskennallisen propagandan käyttämisestä osana vaali- tai kampanjaviestintää. Sekä Trumpin kampanja että Brexit-kampanja ovat yhdistetty Cambridge Analyticaan, nyt huonomaineiseen poliittisen viestinnän konsultointiyritykseen.[37] Trumpin kampanjan kohdalla tämä on tosin vain osa syytöksistä kampanjaa kohtaan (aiheesta lisää luvussa 3.)[38] Puolan PiS-puoluetta on syytetty laajasti bottien käyttämisestä suppressioon ja amplifikaatioon, astroturffaukseen ja algoritmiseen manipulaatioon.[39] Saksassa AFD:tä on syytetty useiden bottikäyttäjien ja verkkojen hyödyntämisestä omien viestien levittämiseen ja voimistamiseen.[40]

2.3. Yksityiset toimijat

Yksityiset tai kaupalliset toimijat muodostavat merkittävän kolmannen toimijan laskennallisen propagandan ekosysteemissä. Ne ovat viestintäyrityksiä, digitaalisten markkinointimenetelmien tai poliittisen viestinnän konsultteja tai muita palveluja tarjoavia kolmannen osapuolen kokonaisuuksia. Niiden asiakkaat voivat usein olla poliittisia kampanjoita, puolueita tai valtiollisia toimijoita.[41]

---

[36] Ibid.

[37] Mm. Risso, L. 2018. *Harvesting Your soul? Cambridge Analytica and Brexit*. The Selected Proceedings of the Symposium. Akademie der Wissenschafter und der Literatur, p. 75-88. https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy., https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html., https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory.

[38]Joseff. K. & Woolley S. 2019. Executive Summary. Teoksessa Joseff. K. & Woolley S *The Human Consequences of Computational Propaganda: Eight Case Studies from the 2018 US Midterm Elections.* Institute for the Future.

[39] Gorwa. R. 2019. Unpacking the Ecosystem of Social Media Manipulation. Teoksessa Woolley, S. & Howard, P. *Computational propaganda: Political Parties, Politicians, and Political Manipulation on Social Media.* New York: Oxford University Press.

[40] Neudert. L. 2019. A Cautionary Tale. Teoksessa Woolley, S. & Howard, P. *Computational propaganda: Political Parties, Politicians, and Political Manipulation on Social Media.* New York: Oxford University Press.

[41] Bradshaw, S. & Howard, P. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Computational Propaganda Research Project.

Palvelut ja niitä tarjoavat yritykset voivat erota toisistaan hyvin merkittävästi. Toimijat voivat yksinkertaisesti myydä laskennallisen propagandan levittämiseen sopivaa ohjelmistoa sekä strategioita tai valmiiksi rakennettuja valetilejä. Ne voivat olla jo tileihin liitettyjä botteja tai kokonaisia bottiverkostoja sekä näiden operoimiseen tarvittavia ohjelmistoja. Kokonaisvaltaisemmat palvelupaketit voivat muodostua pienimuotoisista ja huomaamattomista vaikutuskampanjoista, jotka kenties omaksuvat joitakin astroturffauksen elementtejä, tai ne voivat olla laajamittaisia, organisoituja manipulaatiokampanjoita, joiden tarkoitus on yrittää liikuttaa kokonaista kansakuntaa.[42] Tällöin yritykset tyypillisesti tarjoavat hyvin kehittyneitä profilointi- ja kohdistuspalveluita, kuten psykometriikkaa ja psyops-menetelmiä. Vaikka tällaisten palveluiden toimivuudesta on erimielisyyksiä, on kuitenkin huomattava, että monet lukuisat yritykset tarjoavat näitä palveluita ja väittävät voivansa voittaa vaaleja niiden avulla.

Toisin kuin poliittisten tai valtiollisten toimijoiden motiivit, yksityisten toimijoiden motiivit eivät yleensä ole sinänsä liitettyjä asiakysymyksen tai vaalien lopputulokseen, vaan ne seuraavat enemmän asiakkaiden motiiveja. Laskennallinen propaganda on keino menestyä yrityksenä myymällä omaa erityisosaamistaan, hyvin samankaltaisesti kuin mikä tahansa muukin yritys. Tämä itsessään ei tosin poista niiltä sitä vastuuta tai merkittävää asemaa, joka niillä on sekä ilmiön edistämisessä ja mahdollistamisessa. Toisaalta se kuitenkin tarkoittaa, etteivät ne usein ole sen pahempia (tai parempia) kuin monet muutkaan kyseenalaisilla aloilla toimivat yritykset.

Yksityisten toimijoiden keskeinen rooli korostuukin siten, että ne ovat yhdistävä tekijä poliittisille ja valtiollisten laskennallisen propagandan toimijoiden rajapinnassa. Ne tarjoavat etuja poliittisille puolueille ja valtiollisille toimijoille, mahdollistamalla tietynasteisen etääntymisen kiistanalaisista vaikutusoperaatioista, jotka voisivat johtaa negatiiviseen julkisuuteen tullessaan yleiseen tietoisuuteen. Samalla lukuun ottamatta joitakin merkittäviä ja tunnistettuja valtiollisia toimijoita (kuten Kiina ja Venäjä), niiden kompetenssit ovat sekä jatkuvan kilpailun, innovaation että myös suuren valikoiman takia maailmanluokan huippua, tukien näitä merkittävillä resursseilla ja verkostoilla.

[42] https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Konkreettista yritysten, niiden toimintamallien ja ekosysteemin tutkimusta on toistaiseksi melko vähän. Esimerkiksi laajaa kartoittavaa tutkimusta näistä yrityksistä ei ole toistaiseksi olemassa. Osittain tämä myös vaikeuttaa mahdollisuuksia tehdä selkeää arviota niiden yleisyydestä tai kattavuudesta. Vuonna 2018 kirjoitettu NATO STRATCOM-raportti arvioi sosiaalisen median vaikuttamisen markkinoita kysynnän, tarjonnan ja vaihtoehtojen osalta. Raportti toteaa, että olemassa oleva ekosysteemi on kukoistava ja melko tuottoisa. Toisaalta raportin kirjoittajat korostavat yllättyneisyyttään siitä, miten edullista sosiaalisen median manipulaatio ja siihen liittyvät palvelut ovat. Raportti toteaa myös useiden toimijoiden mainostavan toimintaansa poikkeuksellisen avoimesti, viitaten esimerkiksi helposti yleisimmillä hakukoneilla löydettäviin sivustoihin sekä mainoksiin Googlessa ja Bingissä.[43] Tästä itsessään voidaan päätellä, että palveluille on olemassa ainakin jossain määrin laajat markkinat. Samalla palvelut ovat yllättävän helppoja tavoittaa.

Alan avoimuutta voidaan myös selittää sillä, että vaikka palvelut selkeästi toimivat sosiaalisen median palveluiden käyttöehtojen[44] vastaisesti, jäävät ne silti useissa maissa laillisesti katsoen harmaalle alueelle. Lainsäätäjät eivät useissa tapauksissa ole suoraan puuttuneet tämänkaltaisen toiminnan tai palveluiden laillisuuteen. Tällöin myös näitä palveluja tarjoavat yritykset voivat olla toiminnassaan huomattavan avoimia. Vaikka suuremmilla sosiaalisen median alustoilla saattaisi olla kiinnostusta vaikeuttaa tällaisten yritysten toimintaa tai pyrkiä estämään sitä, laillisesta näkökulmasta niiden toimintaedellytykset ovat ainakin toistaiseksi jossain määrin turvatut.

Tämän takia muun muassa Yhdysvalloissa erilaisia sosiaalisen median manipulaation palveluita tarjoavista yrityksistä on tullut entistä vakiintuneempi, tosin ei vieläkään täysin avoin osa poliittista kamppailua. Luku 3 kokonaisuudessaan kuvaa erilaisia laskennallisen propagandan keinoja, joita myös monet yritykset käyttävät. Esimerkkinä luku 3.4 käsittelee Yhdysvalloissa esille noussutta pink-slime uutisointia ja potemkin-tyylisiä vale-paikallisuutissivustoja. Vaikka itse sivuja on satoja, näistä suurin osa oli mahdollista liittää muutamaan sivustoja rakentavaan kaupalliseen toimijaan.

[43] Singularex. 2018. The Black Market for Social Media Manipulation. NATO Stratcom COE.
[44] Huom. Tyypillisesti käytetty ja vakiintunut englanninkielinen termi ToS tai Terms of Service kuvaa palvelun käyttöehtoja, joihin käyttäjien pitää automaattisesti sitoutua voidakseen käyttää palvelua. Lähteet: https://twitter.com/en/tos, https://www.facebook.com/terms.php

2.4 Alustat

Vaikka Facebook on yhä laskennallisen propagandan ja disinformatiivisten vaikutuskampanjoiden ykköskohde, samat ilmiöt vaikuttavat silti yhtä lailla myös Twitterissä, Youtubessa, Googlessa ja sen eri alapalveluissa, Whatsappissa, Snapchatissa, Tik Tokissa, Redditissä ja useilla erilaisilla foorumeilla ja sosiaalisen median alustoilla.[45] Disinformaation muodot vaihtelevat jossain määrin eri alustoilla sopeutuen alustan erityisominaisuuksiin, piirteisiin ja viestintäkulttuuriin. Samalla eri palveluiden tyypilliset käyttäjät voivat joissakin tapauksissa vaihdella merkittävästi, mikä vaikuttaa luonnollisesti siihen, millaiset toimijat ovat kiinnostuneita alustoista.

Facebookin selkeä etu on sekä sen koossa (laajimmalle levinnyt, eniten käytetty ja suosituin sosiaalisen median alusta) ja sen ominaisuuksissa, jotka tekevät siitä erinomaisen alustan disinformaation levittämiselle. Facebookilla on myös esimerkiksi Twitteriin verrattuna epäsuora etu, joka on sen merkittävä läpinäkyvyyden puute. Twitter on tyypillisesti ollut kohtalaisen avoin, antaen esimerkiksi tutkijoiden käyttää rajapintaansa datan keräämiseen.[46] Tämän rajapinnan kautta tutkijoiden niiden on mahdollista kerätä tietoa julkisista twiiteistä ja analysoida niitä.[47] Vaikka nämä työkalut eivät suurimmaksi osaksi ole täydellisiä taikka ilmaisia, ne kuitenkin tarjoavat tutkijoille mahdollisuuden analysoida Twitterissä toteutuvaa aktiivisuutta sekä seurata sen ilmiöitä. Facebook puolestaan on tässä suhteessa pitkälti musta laatikko eikä tarjoa tutkijoille juuri minkäänlaisia mahdollisuuksia alustalla tapahtuvan aktiivisuuden seurantaan tai analysointiin, lukuun ottamatta joitain harvinaisia poikkeuksia.[48]

Tämä ero Facebookin ja Twitterin välillä on myös eräs syy sille, miksi Facebook houkutella enemmän toimijoita. Koska disinformaatio ja laskennallinen propaganda ovat molemmat merkittävästi tehokkaampia ja itseasiassa jossakin määrin nojaavat siihen, etteivät niiden kohteet tunnista niitä, Facebookilla on merkittävä etu suhteessa

[45] Bradshaw, S. & Howard, P. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation.* Computational Propaganda Research Project.
[46] Twitter tarjoaa erilaisia mahdollisuuksia tutkijoille kerätä Twiittejä sen tarjoamilla API:lla. Tämä tarjoaa tutkijoille mahdollisuuksia observoida Twitterissä tapahtuvaa aktiivisuutta esimerkiksi tiettyjen aihealueiden ympärillä.
[47] https://help.twitter.com/en/rules-and-policies/twitter-api
[48] Poikkeuksena esimerkiksi Yhdysvaltain senaatin 2018 tutkinta Venäjän vuoden 2016 vaalisekaantumiseen Yhdysvalloissa, jonka kanssa useimmat suuret sosiaalisen median alustat tekivät yhteistyötä. Kuitenkin myös tässä tapauksessa Facebookin yhteistyö osoittautui merkittävillä tavoilla puutteelliseksi.

esimerkiksi Twitteriin. Tutkijoiden mahdollisuudet havaita kampanjoita reaaliajassa tai jälkikäteen ovat merkittävästi parempia alustoilla, joissa tutkijoilla on sekä työkaluja että mahdollisuus alustalla tapahtuvan aktiivisuuden tarkkailuun. Se ettei Facebook tarjoa tätä mahdollisuutta, on toimijalle merkittävä etu. Tämä tarkoittaa samalla, että myös valtiollisten vaikutusoperaatioiden havaituksi tuleminen on epätodennäköisempää.

Toisena etuna toimijoiden näkökulmasta on, että Facebookia on tyypillisesti ollut haluttomampi puuttumaan aktiivisiin disinformaatiokampanjoihin. Vaikka se on saanut tästä osakseen merkittävää kritiikkiä, laskennallisen propagandan toimijoiden näkökulmasta tämä on kuin mainos alustan soveltamisen puolesta.[49]

2.4.1 Facebook[50]

Facebook on maailman suurin sosiaalisen median alusta. Sillä on noin 2,6 miljardia aktiivista kuukausittaista käyttäjää.[51] Sen liikevaihto oli yli 70 miljardia dollaria vuonna 2019 (70.6 miljardia) ja 56 miljardia dollaria vuonna 2018.[52] Facebook on kasvattanut sekä aktiivisten käyttäjien määrää että tulostaan tasaisesti vuodesta toiseen. Samalla sen liikevaihdon kasvu on merkittävästi ohittanut käyttäjämäärän kasvun.[53] Käyttäjämääriltään Facebook on myös sen lähimpiä kilpailijoita suhteettomasti suurempi. Esimerkiksi Twitterillä on vain 330 miljoonaa aktiivista kuukausittaista käyttäjää ja

---

[49] Full Fact. 2019. *Report on the Facebook Third Party Fact Checking programme*. https://fullfact.org/media/uploads/tpfc-q1q2-2019.pdf., https://www.business-humanrights.org/en/latest-news/facebook-twitter-allegedly-taking-insufficient-action-to-stop-spread-of-hate-speech-misinformation-through-their-platforms/., https://www.dw.com/en/is-facebook-doing-enough-to-combat-fake-news/a-48608648.

[50] Huom. Lukijan oletetaan tuntevan Facebookin perustoimintaperiaatteet, eikä luku käsittele tätä osuutta sosiaalisen median alustan toiminnasta.

[51] https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[52] https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/

[53] Vuoden 2014 viimeisestä neljänneksestä vuoden 2019 viimeiseen neljännekseen, Facebookin aktiivisten kuukausittaisten käyttäjien (MAU) määrä on noussut noin 78 %.
Samalla aikavälillä sen liikevaihto on nelinkertaistunut, tai kasvanut noin 395 %, ja sen liikevoitto viisinkertaistunut, tai kasvanut noin 500 %. Suhteutettuna sen käyttäjämäärän kasvuun, Facebookin liikevaihto on kasvanut yli viisinkertaisella tahdilla ja liikevoitto merkittävästi yli kuusinkertaisella tahdilla. Tätä kasvua voidaan selittää yksinkertaisesti kasvaneella ja tuottoisammalla mainosmyynnillä, sillä yli 98 % Facebookin liikevaihdosta tulee mainoksista (vuonna 2018 tämä luku oli 98.5 %. Vastaavaa lukua vuodelta 2019 ei ole vielä saatavilla). Tällä on kuitenkin merkittäviä implikaatioita, sillä hyper-kohdennettu mainonta on eräs erityisesti poliittisten toimijoiden käyttämistä laskennallisen propagandan keinoista. Lähteet: (Huom. laskelmat kirjoittajan omia.) Facebook. 2018. *Annual Report*. https://www.annualreports.com/HostedData/AnnualReportArchive/f/NASDAQ_FB_2018.pdf. https://www.statista.com/statistics/277229/facebooks-annual-revenue-and-net-income/., https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-usersworldwide/.,

Facebookin omistamalla Instagramilla aktiivisia kuukausittaisia käyttäjiä on noin 1 miljardi.[54]

Oxfordin Yliopiston Computational Propaganda Project arvioi vuoden 2019 julkaisussaan Facebookin olevan yhä keskeisin alusta disinformaatiolle, laskennalliselle propagandalle sekä vaikutusyrityksille.[55] Muun muassa Yhdysvaltain senaatti tunnisti vuoden 2018 tutkinnassaan Facebookin ylivoimaisesti keskeisimmäksi alustaksi Venäjän sosiaalisen median vaalisekaantumiselle sekä vaikutusyrityksille (tosin myös Instagram, Twitter, Google ja Googlen omistama Youtube näyttelivät merkittäviä rooleja).[56] Senaatin tutkinnan osana toimineet tutkijat nostivat myös esille Facebookin todella hitaan reagoinnin Venäjän disinformaatio-kampanjaan, joka oli saanut jatkua häiritsemättä vuoden 2015 alusta vuoden 2017 loppuun kattaen kokonaisuudessaan noin kolmen vuoden aikaikkunan.[57]

Laskennallinen propaganda on alkanut muodostaa keskeisen osan Facebookin disinformaatiokulttuuria. Se koostuu usein esimerkiksi astroturffauksesta, valeuutisten levittämisestä ja amplifikaatiosta. Toimintaan sisältyy myös käyttäjien häirintää, uhkailemista ja DDoS 2.0:n kaltaisista kohdistetuista automaattisen ylläpidon väärinkäytöksiä sekä mikrokohdistettua mainontaa. Näistä jälkimmäinen on ollut erityisesti poliittisten kampanjoiden (tosin myös kyberjoukkojen ja valtiollisten toimijoiden) suosiossa.

Venäjän vaikutusoperaatiot sen kolmen vuoden analysoidun aktiivisuuden aikana (huomioi, että itse operaatiot alkoivat todennäköisesti jo 2012 ja jatkuvat nykypäivään) keskittyivät pitkälti astroturffaukseen ja valesivujen operoimiseen, joiden kautta se rakensi valheellisia online-persoonia sekä sivustoja. Näiden venäläisten toimijoiden ylläpitämien valesivujen tarkoitus oli vahvistaa yhteiskunnallisia kahtiajakoja jakamalla uutisia muun muassa poliisiväkivallasta, yhteiskunnallisista ongelmista ja ihonväriin

[54] https://www.searchenginejournal.com/social-media/biggest-social-media-sites/#ok
[55] Bradshaw, S. & Howard, P. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Computational Propaganda Research Project.
[56] United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views*. Report of the Select Committee on Intelligence. 116th Congress, 1st. session.
[57] United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views*. Report of the Select Committee on Intelligence. 116th Congress, 1st. session.

liittyvistä haasteista ja käyttämällä dialogia, jonka tarkoitus oli voimistaa sosiaalista vastakkainasettelua.[58] Samalla Facebook on toiminut hyvin merkittävänä osana koronavirus-pandemiaan ja Covid-19 virukseen liittyvän disinformaation levittämisessä. Sekä Kiina että Venäjä ovat käyttäneet sosiaalista mediaa ja erityisesti Facebookia levittääkseen koronavirukseen liittyvää disinformaatiota ja salaliittoteorioita hyödyntäen jo olemassa olevia laajoja lukijakuntia, jotka muun muassa niiden valtiollisilla julkaisuilla on. On myös todennäköistä, että sekä Venäjä että Kiina hyödyntävät jonkinlaisia amplifikaatio-menetelmiä tai bottiverkostoja disinformaation levittämisen tehostamiseksi, vaikka tätä ei toistaiseksi ole varmennettu.[59]

Myös 2016 Iso-Britannian Brexit-kansanäänestyksestä on esitetty voimakkaita epäilyjä siitä, että Venäjä olisi sekaantunut ja yrittänyt vaikuttaa vaaleihin. 2016 Julkaistu tutkimus, joka tarkasteli Twitteriä, huomasi merkittävää bottiaktiivisuutta Twitterissä, keskittyen #Brexit-liikeen tukemiseen.[60] Näitä botteja ei liitetty Venäjään tai toiseen yksittäiseen toimijaan. Heinäkuussa 2020 julkaistu Iso-Britannian raportti, joka tarkasteli Venäjän mahdollista sekaantumista Brexit-kansanäänestykseen, totesi, etteivät Britannian turvallisuuspalvelut olleet tietoisia mahdollisesta vaalivaikuttamisesta, sillä ne eivät olleet tutkineet asiaa tai saaneet määräystä vaalisekaantumisen tutkimisesta, uhan arvioimisesta tai sen torjumisesta.[61] Iso-Britannian kansalliset turvallisuuspalvelut myönsivät kuitenkin, että Venäjä oli ”Iso-Britannian tärkeimpiä ja keskeisimpiä turvallisuusuhkia” ja ”merkittävä kyseenalaistava tekijä kansalliselle turvallisuudelle”.[62]

---

[58] Huom. Tässä yhteydessä vältetty suoraa käännöstä ”rotu-ongelmat” termille ”racial issues” ja sen sijaan puhutaan ”ihonväriin liittyvistä haasteista”. Tämä erityisesti siitä syystä, että termi ’rotu’, viittaa vanhentuneeseen ja selkeän rasistiseen tapaan käsittää erilaisia etnisyyksiä tai ihonvärejä erillisinä ”ihmisrotuina”, tukien selkeästi ei-hyväksyttävää oletusta ”rotujen” välisistä eroista tai arvoista.

[59] Venäjän roolia vuoden 2016 Yhdysvaltain presidentinvaaleissa käsitellään tarkemmin Luvussa 4.1. Venäjän ja Kiinan roolia koronaviruksen ja koronavirus-pandemiaan liittyvän disinformaation suhteen käsitellään Luvussa 4.2.

[60] Howard, P. & Kollanyi, B. 2016. *Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum.* COMPROP, Research Note 2016.1

[61] Merkittävää raportissa on erityisesti se, että se paljastaa, ettei Iso-Britannian valtio ole tarkastellut tai yrittänyt torjua Venäjän vaalisekaantumista kansallisiin vaaleihin tai Brexit-kansanäänestykseen missään määrin, mutta että se siitä huolimatta pitää Venäjää hyvin merkittävänä turvallisuusuhkana ja tunnistaa hyvin sekä Venäjän hybridi-, kyber-, ja sosiaalisen median vaikutusmahdollisuudet. Raportti viittaa siis hyvin selkeästi siihen, ettei Iso-Britannian poliittinen johto halunnut tietää vastausta siihen, sekaantuiko Venäjä Brexit-kansanäänestykseen vai ei.
The UK Parliament. 2020. *Russia*. Intelligence and Security Committee of Parliament, HC 632.

[62] Ibid.

Englannin Parlamentin tekemä, vuonna 2018 julkaistu raportti nostaa esille myös Russia Todayn ja Sputnikin julkaisut edeltäen Brexit-kansanäänestystä. RT ja Sputnik julkaisivat yli 260 artikkelia liittyen Brexit-kansanäänestykseen, tukien voimakkaasti näkemystä, että Britannian tulisi erota EU:sta.[63] RT:n ja Sputnikin Brexit-uutisointi tavoitti hyvin todennäköisesti useita miljoonia käyttäjiä Facebookissa.[64] Johtuen kuitenkin Facebookin toistuvista kieltäytymisistä auttaa tai osallistua tutkintaan, tarjota dataa siihen liittyen tai tehdä millään tavalla yhteistyötä tutkinnan kanssa, tarkkoja arvioita on vaikea arvioida. Viestintäyhtiö 89upin aiheesta tekemä tutkimus aiheesta arvioi kuitenkin, että Venäjän Brexit-äänestykseen liittyvien operaatioiden arvo olisi ollut noin 4 miljoonaa puntaa.[65]

Tässä palaamme myös keskeisimpään haasteeseen sekä aiheesta tehtävän tutkimuksen että Facebookin itsensä suhteen. Facebook on toistuvasti pyrkinyt sekoittamaan aiheesta esitettäviä kysymyksiä, välttelemään, kieltäytymään vastaamasta tai suoraan valehtelemaan useisiin kysymyksiin, tutkintoihin ja haastatteluihin.[66] Tämä on erityisen ongelmallista, sillä kuten todettu, Facebook itse ei jaa dataansa tutkijoiden tai viranomaisten kanssa.[67] Sen käyttämä ”black box”-tyyppinen ratkaisu on hyvin rajoittava, sillä se ei tarjoa tutkijoille juuri minkäänlaisia mahdollisuuksia ilmiöiden tarkkailuun.

Tämä on johtanut myös merkittävään vinoutumiseen laskennallisesta propagandasta ja sosiaalisen median disinformaatiosta tehtävän tutkimuksen kanssa. Kun tutkijoiden on lähes mahdotonta päästä käsiksi Facebookin aktiivisuudesta kertovaan dataan, suurin osa

---

[63] Huom. RT ja Sputnik ovat Venäläisomisteisia ja valtiorahoitteisia uutistoimistoja, joiden tiedetään toimivan suoraan Venäjän valtion alaisuudessa. Lähde: 89up. 2018. *Putin's Brexit? The influence of Kremlin media & bots during the 2016 UK EU referendum*. https://www.slideshare.net/89up/putins-brexit-the-influence-of-kremlin-media-bots-during-the-2016-uk-eu-referendum

[64] Ibid.

[65] Ibid.

[66] Mm. United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views*. Report of the Select Committee on Intelligence. 116th Congress, 1st. session. The UK Parliament. 2020. *Russia*. Intelligence and Security Committee of Parliament, HC 632.Howard, P., Ganesh, B., Dimitra, L., Kelly, J.& Francois, C., 2018. *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* Computational Propaganda Research Project., https://secondaryinfektion.org/, https://www.nytimes.com/2018/11/14/technology/facebook-data-russia-election-racism.html, https://mashable.com/article/facebook-defend-new-york-times-report-russian-meddling/?europe=true https://www.theverge.com/2018/11/27/18114228/facebook-russian-data-harvesting-documents-2014-uk-parliment-six4three, https://www.theverge.com/2017/9/8/16277144/facebook-russian-ads-political-explainer-credibility.

[67] https://theconversation.com/facebooks-data-lockdown-is-a-disaster-for-academic-researchers-94533

tutkimuksesta ei käsittele itse Facebookia. Merkittävästi useammin, tutkimukset keskittyvätkin avoimempiin lähteisiin, kuten Twitteriin, huolimatta siitä, että suurin osa laskennallisesta propagandasta keskittyy Facebookiin.

2.4.2. Twitter[68]

Twitter on sosiaalisen median alustoista laskennallisen propagandan ja disinformaation suhteen tutkituin, tunnetuin ja mahdollisesti parhaiten ymmärretty. Se on kooltaan ja käyttäjäkunnaltaan Facebookiin verrattuna paljon pienempi (arviolta 330 miljoonaa aktiivista kuukausittaista käyttäjää[69]). Toisaalta Twitterin käyttäjät ovat usein nuorempia, paremmin koulutettuja ja poliittisesti aktiivisempia. Twitter on myös useammin poliittisen eliitin käyttämä viestintäväline.[70] Tämä johtaa siihen, että vaikka Twitterillä on vähemmän käyttäjiä, ne voivat laskennallisen propagandan näkökulmasta olla korkeamman arvon käyttäjiä. Tätä tukee jossain määrin myös Twitterin rakenne, joka tekee siitä keskusteluille merkittävästi avoimemman. Useat poliitikot, julkiset virkahenkilöt, organisaatiot ja yritykset ovat alkaneet tehdä julkista viestintää aktiivisesti Twitterin kautta todeten sen tehokkaaksi väyläksi tavoittaa käyttäjiään, asiakkaita tai äänestäjiä. Samalla se tarjoaa näille osapuolille mahdollisuuden osallistua keskusteluun muun muassa muiden poliitikkojen tai asiantuntijoiden kanssa.[71]

Koska Twitter on sekä Facebookia avoimempi (ei vain API:nsa ja datansa kanssa vaan myös rakenteeltaan), se on tehnyt siitä oivallisen paikan bottiverkkojen, valekäyttäjien, amplifikaation ja astroturffauksen kasvualustana. Toisin kuin Facebookissa, jossa käyttäjillä on lähtökohtaisesti 5000 ’kaverin’ rajoitus, Twitterissä käyttäjät voivat seurata tai tulla toisiensa seuraamaksi ilman lukumääräisiä rajoituksia. Facebookissa tarjoaa mahdollisuuden kiertää tämä rajoitus muun muassa luomalla sivuja tai julkisia käyttäjiä,

---

[68] Huom. Lukijan oletetaan tuntevan Twitterin perustoimintaperiaatteet, eikä luku käsittele tätä osuutta sosiaalisen median alustan toiminnasta.

[69] https://www.searchenginejournal.com/social-media/biggest-social-media-sites/#ok

[70] Woolley, S. & Howard, P. 2019. Computational Propaganda Worldwide. Teoksessa Woolley, S. & Howard, P. *Computational propaganda: Political Parties, Politicians, and Political Manipulation on Social Media.* New York: Oxford University Press.

[71] Äärimmäinen esimerkki on Yhdysvaltain Presidentti Donald Trump, joka on usein valinnut käyttää Twitteriä viestintään virka-asioista ja politiikasta. Tämä on johtanut tilanteisiin, jossa uutta tietoa ulko- ja sisäpolitiikan toimista tai kriisitilanteista on saattanut tulla Trumpin Twitterin kautta, ohittaen viralliset väylät ja tiedottaen oman kabinettinsa henkilöitä tai hänen omia virkamiehiään täysistä suunnanmuutoksista muun muassa Twiiteillään. Lähde: https://www.politico.com/news/2019/11/11/trump-instincts-unimpeachable-presidency-ukraine-069015

joihin nämä samat rajoitukset eivät päde, mutta se ei tarjoa tätä mahdollisuutta yksityisille käyttäjille.

Toisena erona alustojen välillä on huomattava, että Facebookissa käyttäjien välisen yhteyden, eli ’kaveri’-pyynnön lähettäminen vaatii tyypillisesti jonkinlaisen yhteyden käyttäjien välillä. Toisaalta Twitterissä kynnys seuraamiseen on matalampi ja mikäli käyttäjätiliä ei ole asetettu yksityiseksi, kuka tahansa voi seurata kyseistä käyttäjätiliä. Tätä selittää myös Twitterin asymmetrinen seuraa-toiminto. Facebookissa ’kaveri’-pyyntö vaatii molempien käyttäjien hyväksynnän, kun taas Twitterissä julkiselle tilille seuraa-toiminto ei vaadi aktiivista hyväksyntää seurattavalta henkilöltä. Tämä johtaa yleisesti erilaiseen ja avoimempaan alustaan, jossa käyttäjien on myös mahdollista tavoittaa suurempia yleisöjä.

Twitterin tarjoama API tarkoittaa myös, että toimintaa Twitterissä on helpompi automatisoida. Se tarjoaa kehittyneemmät ja hienostuneemmat työkalut automatisointiin ja asettaa näin kynnyksen matalammaksi myös koordinoidulle epäautenttiselle toiminnalle.[72] Toisaalta, vaikka useat laskennallisen propagandan termit kuvaavat toimintaa, joka on usein saattanut syntyä Twitterissä (esimerkiksi bottiverkostojen ja valekäyttäjien yleisyyttä Facebookissa on ollut vaikeampi arvioida aiemmassa luvussa havainnollistettujen ongelmien takia), on haastavaa arvioida, ovatko ongelmat todella yleisempiä Twitterin puolella. Koska Twitteristä on tehty enemmän aiheeseen liittyvää tutkimusta, on mahdollista päätyä harhapäätelmään siitä että laskennallinen propaganda ja disinformaatio ovat yleisempiä Twitterissä kuin esimerkiksi Facebookissa. Tämä päätelmä ei kuitenkaan välttämättä pidä paikkaansa, sillä useammat lähteet ovat viitanneet siihen, että Facebook olisi laskennallisen propagandan ja disinformaation ykkösalusta.[73]

[72] Esimerkkinä oheinen linkki joka ohjeistaa yksinkertaisen Twitter-botin rakentamisen kymmenessä minuutissa. https://chatbotslife.com/building-a-news-bot-using-twitter-api-in-10-mins-51cf4eb744b4

[73] Tosin esimerkiksi Yhdysvaltain senaatin tutkinta Venäjän sekaantumiseen 2016 presidentinvaaleissa näytti, että sekä Facebook että Instagram olisivat mahdollisesti tavoittaneet laajempia yleisöjä kuin Twitter. Toisaalta julkaisutiheys Twitterissä oli merkittävästi korkeampi (noin kymmenenkertainen määrä sisältöä). Tämä on kuitenkin vain yksittäinen tapaus eikä edes tämän datan pohjalta voida vetää tarkkoja lopputuloksia sen puuttellisuuden takia. (Näitä puutteellisuuksia avataan tarkemmin luvussa 4.) Lähde: Bradshaw, S. & Howard, P. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation.* Computational Propaganda Research Project.

Twitterissä oleva laskennallinen propaganda ei ole epätyypillistä: Se muodostuu valeuutisista, algoritmisesta manipulaatiosta, astroturffauksesta, amplifikaatiosta, suppressiosta ja disinformaation levittämisestä näiden keinoin. Twitter on hyvin haavoittuvainen bottiverkoille ja boteille. Samalla Twitter-botit ovat helppoja rakentaa ja koordinoida. Seuraajaverkkojen rakentaminen boteille voi myös olla yllättävän yksinkertaista. Grimme ja kumppanit tutkivat bottiverkkojen rakentamista ja seuraajamäärien kasvattamista Twitterissä. He huomasivat, että yksinkertaisesti toisten käyttäjien seuraaminen riitti usein automatisoituun seuraajien saamiseen (Twitterissä käytäntönä on useissa tapauksissa, että seurattu käyttäjä seuraa takaisin seuraajaa. Tällöin molemmat hyötyvät seuraajamäärän kasvamisesta.) Kun bottiprofiilit oli rakennettu yksilöllistetysti yhdistäen seuraamiseen ja takaisinseuraamiseen yksinkertaisen uutistwiittauksen ennalta määrätyistä lähteistä, tutkijat pystyivät saamaan boteille noin 1350 seuraajaa kahdeksassa päivässä. Yhdessä bottiverkko (koostuen 30 tutkijan rakentamasta botista) pystyi tavoittamaan hyvin laajan käyttäjämäärän ja twiitatessaan koordinoidusti se pystyi saamaan puskemansa aiheen ”trendaamaan” saksan top 100-aiheissa.[74]

Tutkimuksessa erityisen keskeistä olivat havainnot siitä, miten helppoa bottien automatisointi Twitterissä oli, kuinka helppoa niille oli saada seuraajia ja miten merkittävän vaikutuksen ne pystyivät saavuttamaan. (Vaikka verkosto oli hyvin pieneksi ja tuore, ne pystyivät tuomaan aiheen saksan top 100 ”trending” listalle.) Tutkimus myös paljastaa erittäin hyvin, miten haavoittuvainen Twitter on koordinoidulle epäautenttiselle käytökselle.

Twitter ilmoitti kesäkuun 2020 alussa poistaneensa 170 000 Kiinan valtion vaikutuskampanjoihin liitettyä käyttäjää. Näistä 24 000 oli ydintilejä ja 150 000 oli näiden voimistamiseen käytettyjä amplifikaatio-botteja.[75] Vaikka näin laajan vaikutuskampanjan vaikutuksia tulee olemaan hyvin vaikea arvioida, voidaan joka tapauksessa kohtuullisen korkealla varmuudella sanoa, että näiden valetilien vaikutukset olivat merkittävästi laajemmat kuin 30 botin bottiverkko. Mikäli kuitenkin 30 botin verkko yksin pystyi manipuloimaan ”trending” listaa Saksan kokoisessa maassa, noin

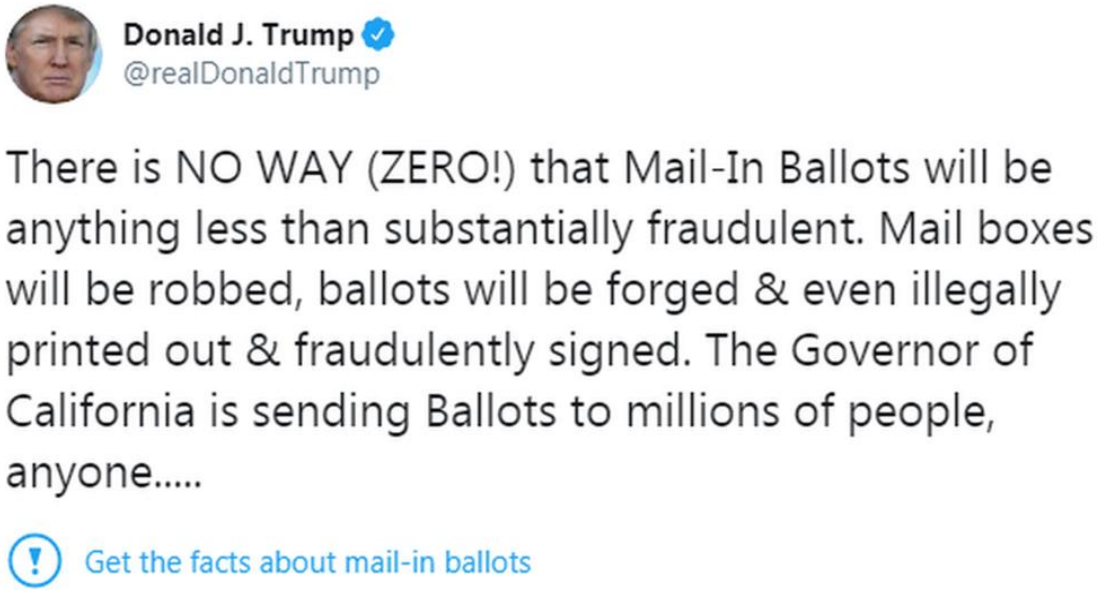
[74] Grimme, C., Preuss, M., Adam, L. & Trautmann, Heike. 2017. *Social Bots: Human-Like by Means of Human Control?*
[75] https://www.theguardian.com/technology/2020/jun/12/twitter-deletes-170000-accounts-linked-to-china-influence-campaign

5000 kertaa suurempi verkosto olisi epäilemättä kykenevä saavuttamaan merkittävästi laajempia vaikutuksia.

Lopuksi merkittäviksi eroiksi Twitterin ja Facebookin välillä voidaan todeta niiden lähestyminen mainontaan viimeisten vuosien aikana. Facebookin kieltäytyessä pitkäaikaisesti puuttumasta poliittisiin mainoksiin ja antaen poliitikkojen avoimesti valehdella niissä, Twitter kielsi vuoden alussa poliittisen mainonnan kokonaan alustallaan eikä salli sitä enää alustalla.[76] Twitter ilmoitti myös 2020 toukokuussa alkavansa liittää merkinnän twiitteihin, joita se epäilee harhaanjohtavasta sisällöstä tai misinformaatiosta.[77] Toukokuun lopussa se liitti tällaisen huomautuksen Yhdysvaltain presidentti Donald Trumpin twiittiin hänen twiitatessaan siitä, miten postitettavat äänestyslomakkeet tulisivat aiheuttamaan merkittäviä määriä äänestyspetoksia.[78] Vaikka mis- ja disinformaatio Twitterissä on todennäköisesti yhtä laajalle levinnyttä kuin Facebookissa, Twitter on ollut valmis kuuntelemaan kansalaisyhteiskunnan ääniä ja pyrkinyt vastaamaan sitä kohtaan asetettuihin vaatimuksiin. Sen viimeisen vuoden aikana ottama aktiivisempi lähestymistapa disinformaatiota vastaan taistelemisen kanssa on usein myös tuonut kritiikkiä niiltä toimijoilta, joita vastaan sen askeleet ovat kohdistuneet. Tätä voidaan kuitenkin pitää positiivisena merkkinä, sillä Twitter on yleisesti ollut melko konservatiivinen tuomioissaan ja pyrkinyt välttämään tarpeetonta ongelmien politisointia.

[76] https://www.nytimes.com/2020/01/09/technology/facebook-political-ads-lies.html, https://www.bbc.com/news/world-us-canada-50243306
[77] https://blog.twitter.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information.html
[78] https://www.bbc.com/news/technology-52815552

Kuva: Donald Trumpin twiitti postitettavista äänestyslomakkeista jonka Twitter on merkinnyt sisältävän mahdollisesti ei-faktuaalista tietoa



Lähde: Donald Trumpin Twitter-tili, www.twitter.com

2.5 Yhteenveto

Luku 2 pyrki johdattamaan lukijan sisään aiheeseen toimija- ja alustakuvauksen kautta. Yleiskuvaukset toimijoista ja ilmiöistä herättävät kuitenkin mielenkiintoisen kysymyksen – Miten vastuu ilmiöstä jakaantuu?

Toimijoiden ja alustojen vastuu ei itsessään ole selkeä kysymys. Tätä ilmiötä on pyritty sekoittamaan, haastamaan ja tekemään epäselväksi monin keinoin. Toimijat itse hyötyvät siitä, että ne voivat toimia hämärällä alueella, välttäen julkisuutta ja kenties edes tietoisuutta olemassaolostaan. Päivänvalolle arka toimiala menestyy yleensä hyvin hämärässä mutta parhaiten tietoisuuden ulkopuolella pilkkopimeässä. Tämä on toisaalta täysin vastakohtaista julkisuuden tai yhteisen edun periaatteen kanssa. Ilman läpinäkyvyyttä ja tietoisuutta ongelmaan puuttuminen on vaikeaa. Laajempi ymmärrys ja tietoisuus toisaalta mahdollistaa vastausten kehittämisen ja vastatoimien muodostamisen.

Sama pätee itse alustoille. Niin kauan kuin kysymys vastuusta ja ongelmista itsessään säilyy epäselvänä, hämäränä ja mahdollisimman hyvin poissa julkisesta tietoisuudesta, sen parempi se on näille toimijoille. Strategia on palvellut hyvin esimerkiksi Facebookin kaltaisia alustoja. Teknologiatietoisuuden ollessa alhaisempi, sosiaalisen median alustat

ovat voineet esittää tyhmää, valehdella tai piilotella ongelmia, sillä lainsäätäjien tietoisuus ongelmista on ollut heikompi.[79] Toisaalta viimeisten vuosien aikana lainsäätäjien tietoisuus teknologiasta ja sen ongelmista on kasvanut. Samalla myös mahdollisuudet ongelmien tunnistamiseen ja niiden ratkaisemiseen ovat ajan myötä parantuneet.[80]

Julkisen tietoisuuden ja lainsäätäjien ymmärryksen kehittyessä myös itse ilmiö alkaa näyttäytymään selkeämpänä. Huolimatta siitä mitä alustat sanovat, pahantahtoisia toimijoita on aina ollut olemassa, kuten niitä aina tulee olemaan. Loppujen lopuksi on kuitenkin itse alustojen vastuulla säädellä sisältöään ja huolehtia palvelujensa turvallisuudesta sekä siitä etteivät pahantahtoiset toimijat voi käyttää niitä hyväkseen. Kysymys vastuusta ja jatkotoimista on itsessään kuitenkin merkittävästi laajempi, minkä takia kysymykseen palataan luvussa 5.

Seuraavaksi alkava luku 3, tapauskuvaus kuvaa kahta todellisen maailman tapausta, antaen esimerkkejä disinformaation ja laskennallisen propagandan käytöstä osana laajaa vaikutuskampanjaa. Näissä tapauksissa näemme, miten disinformaatio pyrkii haastamaan näkemyksiä vastuusta, vaikuttamaan maakuviin sekä manipuloimaan yhteiskuntia. Luku neljä palaa syvempään tarkasteluun laskennallisen propagandan keinoista sekä suorittaa yksityiskohtaisempaa tarkastelua eri laskennallisen propagandan strategioista ja taktiikoista.

3. Tapauskuvaus

Luku 3 keskittyy esittämään yksityiskohtaisesti kaksi tapauskuvausta sekä niiden yhteydessä käytetyt keinot ja keinoja käyttäneiden toimijoiden tavoitteet. Tarkastelun aloittaa viimeisen vuosikymmenen suurin ja eniten näkyvyyttä saanut disinformaation vaikutusoperaatio, Venäjän vaalisekaantuminen Yhdysvaltain 2016 presidentinvaaleihin. Tapauksesta suoritettu senaatin tutkinta paljasti myös kuvan merkittävästi laajemmasta vaikutusoperaatiosta, jonka historia ulottui taaksepäin edeltäen 2016 vaaleja usealla vuodella ja kasvaen skaalassa sen jälkeen. Toisena tapauksena seuraa vuonna 2020 alkanut maailmanlaajuinen koronaviruspandemia, joka on aktivoinut pahantahtoisten toimijoiden disinformaatiokampanjat ennennäkemättömällä tavalla. Vaikka pandemia on

[79] Hyvänä esimerkkinä vuoden 2018 kuuleminen Yhdysvaltain senaatille, jossa Facebookin perustaja ja toimitusjohtaja Mark Zuckerberg oli kuultavana. https://www.youtube.com/watch?v=n2H8wx1aBiQ
[80] https://www.nytimes.com/2020/07/30/technology/big-tech-ceos.html

yhä käynnissä ja ilmiön koko laajuutta ei voida vielä arvioida, ei ole epäilystäkään siitä, että kyseessä saattaa olla jopa Yhdysvaltain vaalivaikutusta laajempi operaatio. Samalla sen haitat ja vaikutukset voivat olla Yhdysvaltain tapaukseen verrattuna moninkertaiset.

Johdanto tapauksiin

Mahdollisesti eniten näkyvyyttä saanut laskennallisen propagandan ja informaatiosodankäynnin tapaus oli Venäjän yritys vaikuttaa Yhdysvaltojen vuoden 2016 presidentinvaaleihin käyttämällä sosiaalista mediaa disinformaation levittämiseksi, olemassa olevien jakolinjojen syventämiseksi sekä jo valmiiksi kaltoinkohdeltujen ryhmien vahingoittamiseksi ja eristämiseksi.[81]

Vuonna 2016 epäilykset Venäjän yrityksistä auttaa silloista republikaanisen puolueen presidenttiehdokas Donald Trumpia ja vahingoittaa demokraattisen presidenttiehdokas Hillary Clintonin mahdollisuuksia laukaisivat tutkinnan Venäjän sekaantumisesta vuoden 2016 vaaleihin.[82]

Yhdessä Yhdysvaltojen tiedusteluvirastojen kanssa ja kolmannen osapuolen tutkijoiden avustamana Yhdysvaltojen senaatti suoritti noin vuoden mittaisen tutkinnan Venäjän toimista. Kaksiosainen raportti sekä sen valmistelusta julkaistut tutkimukset vahvistivat epäilyt, mutta paljastivat tämän lisäksi monivuotisen disinformaatio-operaation, joka oli pyrkinyt vaikuttamaan yhdysvaltalaisten mielipiteisiin ja asenteisiin, alkaen mahdollisesti jo vuodesta 2012.[83] Löydökset perustuvat sosiaalisen median alustojen, Facebookin, Twitterin ja Googlen jakamiin tietokantoihin, jotka koskivat näiden organisaatioiden tunnistamia venäläisiä valetilejä ja käyttäjiä. Nämä toimijat ja tilit oli liitetty vahvasti Kremlin tukemaan Internet Research Agencyyn tai IRA:han.[84]

---

[81] United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views*. Report of the Select Committee on Intelligence. 116th Congress, 1st. session.

[82] Mm. https://www.theguardian.com/us-news/2016/dec/10/cia-concludes-russia-interfered-to-help-trump-win-election-report., https://www.theatlantic.com/politics/archive/2016/12/the-senate-will-investigate-russian-election-interference/510377/

[83] Mm. DiRestra, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. 2020. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge., Howard, P., Ganesh, B., Dimitra, L., Kelly, J.& Francois, C., 2018. *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* Computational Propaganda Research Project., United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views.* Report of the Select Committee on Intelligence. 116th Congress, 1st. Session.

[84] Ibid.

Tapauskuvaus pohjautuu Yhdysvaltain senaatin omaan tutkintaan ja sen tekemiin löytöihin sekä tutkinnan tueksi tuotettuihin kahteen itsenäiseen raporttiin. On huomattava, että vaikka Yhdysvaltain senaatti on poliittinen elin ja se oli tutkimuksen aikana republikaanijohtoisen enemmistön alaisuudessa, raportin tuloksia voidaan pitää pitkälti neutraaleina. Ne pohjaavat voimakkaasti Yhdysvaltain tiedusteluviranomaisten sekä kahden luotetun ja hyvin tunnetun itsenäisen tutkimusryhmän työhön. Tutkimusraportin tulokset eivät myöskään ole linjassa republikaanisen puolueen laajemman agendan kanssa sen johtopäätösten osoittaessa voimakkaasti Venäjän sekä sekaantuneen vaaleihin että suosineen viestinnässään silloista presidenttiehdokas Trumpia. Myös erikoistutkija Robert Muellerin Yhdysvaltain oikeusministeriölle kirjoittama raportti tukee senaatin raportin löydöksiä ja voimistaa näin niiden uskottavuutta.[85] Samalla raportin tunnistama keskeinen toimija, IRA, on liitetty disinformaatio-operaatioihin ja laskennalliseen propagandaan monien itsenäisten tutkimusten, uutisointien ja raportoinnin yhteydessä. Tämä antaa uskottavuutta myös raporttien esittämälle toimijakuvaukselle.

Toisena tapauskuvauksena vuosi 2020 on tuonut mukanaan myös maailmanlaajuisen koronaviruspandemian. Koronavirus on vaatinut 750 000 uhria tähän päivään mennessä (01.08.2020) eikä pandemian loppumisesta ole toistaiseksi selkeää ennustetta.[86] Kiinasta lähtöisin olevan viruksen leviäminen on johtanut laajojen disinformaatio-kampanjoita laukaisemiseen, joiden ajajana muun muassa Venäjällä ja Kiinalla on ollut hyvin merkittävä rooli.[87] Ilmiö on monissa suhteissa testannut yhteiskuntamme resilienssiä sekä kykyämme selviytyä maailmanlaajuisesta pandemiasta ja systemaattisesti levitetystä ja kohdistetusta disinformaatiosta pandemiaan liittyen. Monissa tapauksissa yhteiskuntamme ovat valitettavasti olleet kykenemättömiä vastaamaan haasteeseen.

---

[85] Special Counsel Robert S. Mueller. 2019. *Report on The Investigation Into Russian Interference in the 2016 Presidential Election. Volume I of II*. U.S. Department of Justice.
[86] https://www.worldometers.info/coronavirus/?
[87] OECD. 2020. *Combatting COVID-19 disinformation on online platforms.* https://read.oecd-ilibrary.org/view/?ref=135_135214-mpe7q0bj4d&title=Combatting-COVID-19-disinformation-on-online-platforms., European Commission. 2020. *Tackling Coronavirus Disinformation.* https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_en. https://www.bbc.com/news/blogs-trending-51271037

Luku 3.1 tarkastelee Venäjän monivuotisia disinformaatio-operaatioita Yhdysvalloissa keskittymällä erityisesti IRA:n toimintaan. Luku havainnollistaa, miltä vieraaseen valtioon kohdistuva todellisen maailman disinformaatio-operaatio näyttää. Luku tekee tämän tarkastelun seitsemän Venäjän operaatioita käsittelevän alaluvun kautta. Valitut alaluvut ovat 3.1, toiminnan aikajana, 3.1.2, IRA:n tavoitteet, 3.1.3, presidenttiehdokkaan valitsemiseen sekä vaaleihin vaikuttaminen, 3.1.4 irtautumisliikkeiden tukeminen ja isolationismin vahvistaminen, 3.1.5 sosiaalisten kahtiajakojen syventäminen, 3.1.6, Tapaus Black Matters US ja 3.1.7, toimijoiden kehitys.

Nämä näkökulmat toiminnan tarkasteluun on valittu tapauksesta kokonaiskuvan muodostamiseksi. 3.1.3, 3.1.4, 3.1.5 ja 3.1.7 on sisällytetty, sillä ne kuvaavat IRA:n operaation keskeisimpiä tavoitteellisia suuntia. Luku 3.1.6, joka havainnollistaa IRA:n toimintaa tarkastelemalla sen ylläpitämää Black Matters US sivustoa ja liikettä. Black Matters US toimii erinomaisena esimerkkinä IRA:n toiminnasta, sillä sen ekosysteemi oli kokonaisuutena hyvin laaja ja monipuolinen, vaikkei se ollutkaan seuraajamäärältään IRA:n sivustoista merkittävin. Samalla se myös havainnollistaa, miten keskeisen kohteen Afro-amerikkalaiset ja tummaihoinen kulttuuri muodostivat Venäjän ja IRA:n operaatiolle.

Luku 3.2 tarkastelee koronavirukseen liittyvää disinformaatiota sekä toimijoita disinformaation taustalla. Se on tapaustarkasteluna jossain määrin yleisluontoisempi nostaen esille maakohtaisina toimijoina erityisesti Venäjän ja Kiinan. Lukua täydentää luku 3.3, joka harkitsee disinformaation vaikutuksia ja seurauksia pandemian aikana.

Käsiteltävät tapaukset valittiin niiden yhteiskunnallisen impaktin ja merkittävyyden vuoksi. Koronaviruksen yhteydessä leviävä disinformaatio edustaa aitoa terveysuhkaa, jonka WHO on ilmiönä nimennyt infodemiaksi. Venäjän vaikutusoperaatiota Yhdysvalloissa voidaan pitää esimerkkinä poikkeuksellisen edistyneen toimijan informaatiosodankäynnin sovellutuksesta, havainnollistaen mitä taitavan toimijan on mahdollista saada aikaan. Koska sen käyttämät keinot ovat hyvin yleisiä ja laajasti sovellettuja, se tarjoaa kehyksen myös eri toimijoiden disinformaatio- ja vaikutuskampanjoiden tarkastelemiseen muualla. Ymmärtämällä Venäjän operaatioita ja toimintaa Yhdysvalloissa on mahdollista ymmärtää myös monia muita toimijoita muissa samankaltaisissa tilanteissa.

3.1. IRA:n vaikutusoperaatiot Yhdysvalloissa

Vuoden 2016 vaalisekaannusepäilykset käynnistivät tutkinnan Venäjän sekaantumisesta vuoden 2016 Yhdysvaltojen presidentinvaaleihin.[88] Senaatin ohjaama tutkinta paljasti laajalle levinneitä, monivuotista informaatio-operaatiota, jotka IRA itse tunnistaa informaatiosodankäynniksi.[89] Ensimmäiset löydökset, jotka viittaavat toiminnan alkamiseen yltävät vuodelle 2012. Tästä eteenpäin ne kasvoivat tasaisesti vuoteen 2018, jolloin Yhdysvaltain senaatin tutkinta johti alustojen toimiin niitä vastaan. Useat lähteet ovat kutenkin osoittaneet operaatioiden olevan yhä aktiivisia ja kasvavan valmistautuessa vuoden Yhdysvaltojen presidentinvaaleihin 2020.[90]

Vaikka alun perin senaatin tutkimus alun perin keskittyi vain Venäjän sekaantumiseen vaaleihin, se onnistui löytämään todisteita merkittävästi suuremmasta operaatiosta, jonka tarkoitus selkeästi ylitti yksinkertaisen vaalisekaantumisen.[91] Senaatin komitean kaksiosaisen raportin ensimmäinen osa käsittelee Venäjän kyberhyökkäyksiä Yhdysvaltojen vaalijärjestelmiä kohtaan keskittyen erityisesti vaalien infrastruktuuriin ja järjestelmiin. Samalla se sisältää tietoa virkahenkilöihin, poliitikkoihin sekä yksityisyrityksiin kohdistuneista Venäläis-lähtöisistä hyökkäyksistä.[92] (Katso esimerkiksi luvut 4.7 ja 4.8.) Äänestysinfrastruktuurin osalta raportti kuitenkin toteaa, että tietovarkauksia lukuun ottamatta, hyökkäykset eivät olleet onnistuneita ja että Venäjä ei onnistunut vaikuttamaan kriittiseen äänestysinfrastruktuuriin tai sen prosesseihin. [93]

---

[88] Mm. https://www.theguardian.com/us-news/2016/dec/10/cia-concludes-russia-interfered-to-help-trump-win-election-report., https://www.theatlantic.com/politics/archive/2016/12/the-senate-will-investigate-russian-election-interference/510377/.

[89] Special Counsel Robert S. Mueller. 2019. *Report on The Investigation Into Russian Interference in the 2016 Presidential Election. Volume I of II.* U.S. Department of Justice.

[90] Howard, P., Ganesh, B., Dimitra, L., Kelly, J.& Francois, C., 2018. The IRA, Social Media and Political Polarization in the United States, 2012-2018. Computational Propaganda Research Project., https://www.theguardian.com/technology/2019/oct/21/facebook-us-2020-elections-foreign-interference-russia

[91] United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views.* Report of the Select Committee on Intelligence. 116th Congress, 1st. Session.

[92] United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 1:* Russia's Use of Social Media with Additional Views. Report of the Select Committee on Intelligence. 116th Congress, 1st. Session.

[93] Ibid.

Raportin toinen osa kuvaa miten Venäjän hyödynsi sosiaalista mediaa osana vaikutusoperaatiotaan. Tämä osuus raportista keskittyy erityisesti IRA:n toimintaan, joka oli päätoimisesti vastuussa sosiaalisen median kautta suoritettavista operaatioista.[94]

Raportit ja niiden tueksi kirjoitetut tutkimukset perustuvat pääasiassa internetin ja sosiaalisen median jättien, Googlen, Facebookin ja Twitterin vapaaehtoisesti palveluistaan jakamiin tietokantoihin. Nämä tietokannat eivät ole julkisesti saatavilla ja ne keskittyivät palveluiden itse tunnistamiin, IRA:han liitettyihin sivustoihin, käyttäjiin ja sivuihin. Ne sisälsivät tietoa muun muassa Facebookin, Instagramin, Twitterin, Youtuben, Google Adwordsin, Google+ ja Googlen sivustoista sekä palveluista.

Tietokannoissa itsessään oli suuria eroja eri alustojen välillä. Vaikka osa datasta oli koneluettavassa muodossa ja näin tutkijoille yksinkertaisesti käsiteltävissä, jotkin toimijat, kuten Google, toimittivat hyvin puutteellisia tietokantoja. Osa näistä tiedoista olivat myös hyvin rajallisia, tallennettuja ei-koneluettavaan muotoon ja sisältäen useissa tapauksissa lukuisia duplikaatteja tai tutkinnan kannalta selkeästi epäolennaisia asioita.[95]

Senaatin raportin tueksi työstetyt kaksi merkittävintä tutkimus-raporttia olivat New Knowledgen *The Tactics & Tropes of the Internet Research Agency* sekä Computational Propaganda Research Projectin *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* Molemmat raporteista käsittelevät IRA:n toimintaa ja muodostavat toisiaan tukevan kuvan. Computational Propaganda Research Projectin raportti keskittyy voimakkaammin monialustaiseen toimintaan ja IRA:n operaation kokonaiskuvaan. New Knowledgen raportti puolestaan käsittelee erityisesti IRA:n käyttämiä taktiikoita ja keinoja sen eri alustoilla. Molemmat raporteista olivat ensimmäisiä kattavan kokonaiskuvan antavia tieteellisiä julkaisuja aiheesta ja tarjoavat valaisevan läpileikkauksen IRA:n toiminnasta viimeisten vuosien aikana.

[94] United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 2: Russia's Use of Social Media with Additional Views.* Report of the Select Committee on Intelligence. 116th Congress, 1st. Session.
[95] DiRestra, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. 2020. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge.

Raporttien keskeisin löydös on IRA:n operaation kattavuus, pitkäjänteisyys ja laajuus. Raportti sekä senaatin tutkinta tunnistavat kolme selkeää ja toisistaan erillistä muotoa Venäjän vaalisekaantumiselle. Nämä muodot olivat:

1) Verkkoon liitettyjen äänestysjärjestelmien hakkerointi sekä virkamiehiin ja äänestystietokantoihin kohdistetut tietohyökkäykset.
2) GRU:n[96] suorittama kyberhyökkäys demokraattista puoluetta kohtaan, joka johti merkittävään tietovarkauteen sekä myöhemmin presidenttiehdokas Hillary Clintonin kampanjan sähköpostien vuotamiseen Wikileaks-sivustolle.
3) Laajamittainen ja pitkäkestoinen vaikutusoperaatio, joka kohdistui Yhdysvaltain kansalaisiin hyödyntäen erilaisia koordinoituja laskennallisen propagandan ja disinformaation menetelmiä.[97]

Molemmat raportit käsittelevät pääasiassa Venäjän vaikutusoperaatiota eli kolmatta kohtaa. Sekä senaatin oma raportti että Yhdysvaltain oikeusministeriön erikoistutkijan Robert Muellerin raportti käsittelee myös kohtia 1 ja 2.[98] Luku 3.1 keskittyy erityisesti käsittelemään IRA:n operaatiota sekä Venäjän käymää monivuotista vaikutusoperaatiota eikä käsittele merkittävissä määrin Venäjän hyökkäyksiä äänestysinfrastruktuuriin tai GRU:n kyberhyökkäyksiä demokraattista puoluetta ja silloista presidenttiehdokas Hillary Clintonia vastaan. (Katso muun muassa luvut 4.7 Doksaus tai 4.8 DDoS-hyökkäykset.)

3.1.1. Aikajana ja aktiivisuus

IRA aloitti toimintansa Yhdysvalloissa aikaisin vuonna 2012, jolloin se alkoi kohdistamaan disinformaatiota äänestäjiin. IRA aloitti kampanjansa käyttäen pitkälti samoja metodeja, joita se oli kohdistanut aiemmin sekä omiin kansalaisiinsa että Itä-Euroopassa oleviin naapurimaihin. Osa IRA:n jo 2012 aktivoimista Yhdysvalloissa englannin kielellä julkaisevista käyttäjistä olivat aluksi uudelleenkohdistettuja tilejä, joita oli aiemmin käytetty disinformaatio-operaatioissa muissa yhteyksissä. Esimerkiksi pieni

[96] GRU – Venäjän asevoimien sotilastiedustelun keskuselin.
[97] Howard, P., Ganesh, B., Dimitra, L., Kelly, J.& Francois, C., 2018. *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* Computational Propaganda Research Project., DiRestra, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. 2020. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge
[98] Special Counsel Robert S. Mueller. 2019. *Report on The Investigation Into Russian Interference in the 2016 Presidential Election. Volume I of II*. U.S. Department of Justice., United States Senate. 2018. *Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election. Volume 1: Russian Efforts Against Election Infrastructure with Additional Views*. Report of the Select Committee on Intelligence. 116th Congress, 1st. session.

osa uudelleenkohdistettuja käyttäjiä oli aiemmin indonesialaiselle käyttäjäpohjalle kohdistettuja vain indonesian kielellä operoivia tilejä.[99]

On myös huomattava, että raporttien käytössä ollut data alkaa pääasiassa vuodesta 2014 tai 2015, lukuun ottamatta Twitterin jakamaa dataa, joka alkaa vuodesta 2009. Täten vaikka IRA:n tiedetään aloittaneen joitakin operaatioita jo vuonna 2012, näiden täyttä kokoa ennen vuosia 2014 ja 2015 on vaikea arvioida puutteellisuuksien vuoksi. Toisena rajoitteena datalle on huomattava, että vaikka Google vastasi tietopyyntöihin, sen toimittamat tietokannat olivat pitkälti hyödyttömiä. Tämä johtui siitä, että se ei sisällyttänyt metadataa videoihin, sen toimittama data oli puutteellista eikä sisältänyt riittävää kontekstia johtopäätösten tekemiseen niiden. Tämän lisäksi suurin osa datasta oli ei-koneluettavassa muodossa. Tästä syystä myös merkittävä osa analyysistä keskittyy Twitterin, Instagramin ja Facebookin sisältöihin.[100]

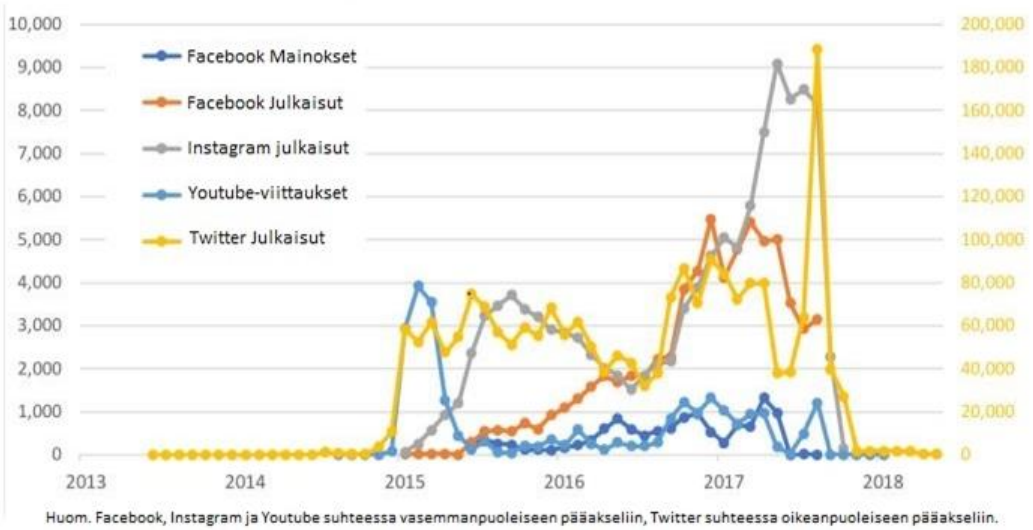
IRA:n aktiivisuus lähti nousemaan merkittävästi vuodesta 2015 eteenpäin. Aktiivisuus saavutti suurimmat piikkinsä vuoden 2017 loppupuolella.[101] Dataseteissä aktiivisuus päättyy täysin vuoteen 2018, johtuen siitä, että tässä kohtaa palvelut joko poistivat tai lakkauttivat ne tilit, jotka ne datasetissä olivat tunnistaneet IRA:n käyttämiksi. Tämä toisaalta ei tarkoita että IRA:n toiminta olisi pysähtynyt. Ensiksikin on mahdollista, että organisaatioilla oli tilejä, joita palvelut eivät tunnistaneet tai halunneet tunnistaa (Facebook, Google tai Twitter eivät jakaneet tietoa siitä, miten tilit oli tunnistettu, joten tätä on mahdoton arvioida.)

Toisena, vaikka kaikki Yhdysvaltojen operaation yhteydessä käytetyt tilit olisi lakkautettu, IRA voisi joko uudelleenohjata olemassa olevia toisissa yhteyksissä käytettyjä tilejään Yhdysvaltain sosiaaliseen mediaan (kuten se teki aloittaessaan operaationsa 2012) tai vain korvata menetetyt tilit uusilla tileillä. Huomioiden myös, että jaettujen datasettien mukaan aktiivisuus on vuosittain noussut tasaisesti, saavuttaen merkittävän huipun vuonna 2017, ei ole mitään syytä uskoa, että IRA lakkauttaisi operaationsa tämän jälkeen. Samalla tiedusteluviranomaiset ovat varoittaneet Yhdysvaltain kongressia Venäjän sekaantumisesta vuoden 2020 vaaleihin[102] ja IRA:n

[99] Ibid.
[100] Ibid.
[101] Ibid.
[102] https://www.nytimes.com/2020/02/20/us/politics/russian-interference-trump-democrats.html

aktiivisuudesta vuodesta 2018 eteenpäin on löydetty merkittävä määrä todistusaineistoa.[103] Myös senaatin tutkinnan tueksi tuotetut raportit arvioivat IRA:n toiminnan sekä operaatioiden aiheuttaman uhan yhä aktiiviseksi ja jatkuvaksi. [104]

Kuvio 1: IRA:n poikkialustainen aktiivisuus vuosina 2014–2018



IRA:n poikkialustainen aktiivisuus vuosina 2014–2018.[105]

Tarkasteltaessa IRA:n aktiivisuuspiikkejä,[106] voidaan huomata, että useat Yhdysvaltojen merkittävät poliittiset tapahtumat vastasivat ja selittävät piikkejä IRA:n mainos- tai julkaisuaktiivisuudessa. Nämä nousut aktiivisuudessa ovat erityisen merkittäviä esimerkiksi presidentinvaalien esivaalien väittelyiden yhteydessä, kuten demokraattien kolmannen esivaalin ja republikaanien kuudennen esivaalin kohdalla (tammikuussa 2016), kaikkien presidenttiehdokkaiden väittelyiden kohdalla (Syksyllä 2016), presidentinvaalipäivänä sekä presidentinvaaleja seuranneen Venäjän sekaantumiseen liittyvän tutkinnan päivinä (29. ja 30. päivä marraskuuta.)[107]

Nämä tapahtumat eivät yksin riitä selittämään kaikkia piikkejä erityisesti mainosaktiivisuuden yhteydessä ja on todennäköistä, että näitä muutoksia ovat ajaneet myös muut strategiset tavoitteet. Useiden Yhdysvaltojen merkittävien poliittisten

[103] Kim, Y., 2020. *New Evidence Shows how Russia's Election Interference has Gotten More Brazen.* Brennan Center
[104] DiRestra, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. 2020. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge.
[105] Howard, P., Ganesh, B., Dimitra, L., Kelly, J.& Francois, C., 2018. *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* Computational Propaganda Research Project.
[106] Ibid.
[107] Ibid.

tapahtumien yhteydessä on kuitenkin nähtävissä selkeitä korrelaatioita korkeisiin mainospiikkeihin, jotka ovat voineet päivittäisellä tasolla tarkoittaa nousua esimerkiksi kymmenkertaista nousua mainosaktiivisuudessa. (Katso luku 4.10, joka käsittelee sosiaalisen median mainontaa ja mikrokohdennusta laskennallisen propagandan keinona.)

3.1.2. IRA:n tavoitteet

IRA:n vaikutus- ja disinformaatiokampanjan tavoitteet voidaan purkaa useisiin eri kategorioihin. Sen keskeisimmät tavoitteet olivat kuitenkin:

- Vaikuttaa Yhdysvaltain 2016 presidentinvaaleihin sekä presidenttiehdokkaiden valintaan.
- Olemassa olevien sosiaalisten kahtiajakojen syventäminen kohdistamalla viestintää strategisesti valittuihin ryhmiin.
- Äänestämisaktiivisuutta laskemaan tarkoitetut toimet tiettyjä ryhmiä kohtaan
- Kirjaimellisten irtautumisliikkeiden vahvistaminen ja Yhdysvaltojen isolationalismi[108]

Näitä valintoja perustellaan luvun 3.1 tulevissa luvuissa.

3.1.3. Presidenttiehdokkaan valintaan sekä presidentinvaaleihin vaikuttaminen

IRA pyrki vaikuttamaan sekä republikaanisen että demokraattisen puolueen presidenttiehdokkaan valintaan. Republikaanisen puolueen ehdokasnimitys-prosessin aikana IRA pyrki tukemaan Donald Trumpia ja hyökkäämään hänen kilpakumppaneitaan kohtaan julkaisemiensa sisältöjen kautta. Samanaikaisesti se teki useita Hillary Clintonia kohtaan hyökkääviä julkaisuja tuottaen negatiivista kuvaa Clintonista julkaisuissaan. Se myös yhtäaikaisesti tuotti sisältöjä, jotka kannattivat Jill Steinin ja Bernie Sandersin ehdokkuutta demokraattisen puolueen presidenttiehdokkaaksi. IRA jatkoi viestintäänsä myös ehdokasnimitysten jälkeen ja keskittyi tänä aikana pitkälti tukemaan Trumpin ja vastustamaan Clintonin ehdokkuutta.[109]

---

[108] DiRestra, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. 2020. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge

[109] Ibid.

Osana operaatiota olivat myös useat erityisesti Clintonin kannattajiin kohdistetut äänestysaktiivisuutta laskemaan tarkoitetut vaalimainokset ja julkaisut. Nämä julkaisut kohdistuivat erityisesti Yhdysvaltain alkuperäiskansoihin, afroamerikkalaisiin, LGBT+ ryhmiin sekä muslimeihin. Viestien tarkoitus oli vakuuttaa näitä kannattajia siitä, ettei Clinton välittänyt vähemmistöryhmistä, trans-henkilöiden tai seksuaalivähemmistöjen oikeuksista eikä edustanut vasemmistolaisia arvoja.

Viestit pyrkivät yleisesti luomaan kuvan siitä, että näiden ryhmien tai niiden oikeuksista välittävien ihmisten olisi parempi jättää äänestämättä, samalla toistamalla dialogia, jonka mukaan heidän äänensä ollut tärkeä tai merkityksellinen. Julkaisut myös ehdottivat, että heidän tulisi äänestää toista ehdokasta kuin Clintonia.[110] Näiden lisäksi IRA myös pyrki aiheuttamaan sekaannusta äänestämiseen liittyen, suorittaen esimerkiksi Twitterissä ’tekstaa äänestääksesi’-huijauksia, levittäen väärää tietoa äänestyskäytännöistä, äänestystavoista, äänestyspaikoista sekä äänestyspäivästä.[111] IRA toteutti tämän olemassa olevien valesivujensa kautta, sekä luomalla muita virkahenkilöitä ja julkisia toimielimiä esittäviä sivustoja. (Luku 4.5 sisältää lisää tietoa astroturffauksesta)

3.1.4. Irtautumisliikkeiden tukeminen ja isolationismin vahvistaminen

Sosiaalisen kahtiajaon lisäksi IRA pyrki myös luomaan hyvin konkreettisia kahtiajakoja tukemalla Brexitin ja #Brexitin mukaan nimettyjä #Texit ja #Calexit liikkeitä, jotka esittivät, että näiden osavaltioiden tulisi erota Yhdysvaltojen liittovaltiosta. IRA käytti esimerkiksi 2016 kesäkuussa tapahtunutta #Brexit äänestystä saadakseen näkyvyyttä ja julkisuutta Texasin eroamista kutsuville liikkeille, pyrkien samalla tukemaan isolationalistista irtautumisajattelua ja Yhdysvaltojen vetäytymistä maailmanpolitiikasta.[112]

Paikallisella tasolla IRA tuki mellakoita sekä kokoontumisia, joiden tarkoitus oli vetää huomiota erilaisiin ongelmiin ja ruokkia liittovaltioon kohdistuvaa tyytymättömyyttä. Se julkaisu osavaltioissa sisältöjä, jotka pyrkivät korostamaan alueellisia kulttuurieroja ja kyseenalaistamaan osavaltioiden välistä yhtenäisyyttä. IRA myös pyrki vetämään

[110] Ibid.
[111] Howard, P., Ganesh, B., Dimitra, L., Kelly, J.& Francois, C., 2018. *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* Computational Propaganda Research Project.
[112] Ibid.

huomiota ja protestoimaan Amerikan konfederaation patsaiden ja muistomerkkien poistamista vastaan.[113]

3.1.5. Sosiaalisten kahtiajakojen syventäminen

IRA:n keskeisin tavoite oli kuitenkin olemassa olevien sosiaalisten kahtiajakojen syventäminen eri ryhmien välillä. IRA pyrki polarisoimaan yhteiskuntaa ja keskustelua synnyttämällä tyytymättömyyttä ja lietsomalla vihaa, pelkoa sekä ryhmäajattelua. IRA tunnisti potentiaaliset kohdeyleisönsä tehokkaasti ja tuotti erilaisia, tehokkaasti kohdistettuja sisältöjä eri sivujensa kautta. Se tuotti aktiivisesti sisältöä sekä poliittisesti vasemmalla että oikealla puolella oleville ryhmille, uskonnollisille ryhmille (kuten muslimit ja kristityt), sekä erilaisille sosiaalisille tai etnisille vähemmistöryhmille. IRA myös kohdisti poikkeuksellisen määrän resursseja afroamerikkalaisiin, jotka olivat yksi sen merkittävimmistä valitsemista kohderyhmistä.[114]

Viestinnässään IRA keskittyi pitkälti sosiaalisiin ongelmiin, tosin joukossa oli myös muita teemoja. Aiheet kattoivat ainakin seuraavat osa-alueet:

- Afroamerikkalaiset, tummaihoinen kulttuuri, yhteisö, sekä Black Lives Matter-liike
- Blue Lives Matter-liike, poliiseja tukeva sisältö
- Pakolaisvastainen, maahanmuuttomyötäinen
- Eteläinen kulttuuri (Amerikan konfederaatio)
- Eroamisliikkeet
- Muslimien kulttuuri, yhteisö, ylpeys identiteetistä
- Kristittyjen kulttuuri, yhteisö, ylpeys identiteetistä
- LGBT kulttuuri, yhteisö, ylpeys identiteetistä
- Amerikan alkuperäiskansojen kulttuuri, yhteisö, ylpeys identiteetistä
- Meemi ja ”red pill”-kulttuuri[115]
- Isänmaallisuus sekä teekutsuliikkeen kulttuuri
- Liberaali ja feministinen kulttuuri
- Veteraanien ongelmat
- Aseenkanto-oikeudet, perustuslain toisen pykälän suojelu

---

[113] Ibid.
[114] Ibid.
[115] “Red Pill” viittaa alun perin 1999-julkaistusta Matrix-elokuvasta kehittyneeseen meemiin. Nykyisessä kontekstissa ”red pill culture” tarkoittaa voimakkaasti misogyynistä käsitystä naisista sekä naisten ja miesten välisistä suhteista. Katso aiheesta lisää: https://www.theguardian.com/technology/2016/apr/14/the-red-pill-reddit-modern-misogyny-manosphere-men, https://www.urbandictionary.com/define.php?term=the%20red%20pill

- Trumpin kannustus, Clintonin vastustus
- Bernie Sandersin ja Jill Steinin kannustus
- Syyria ja ISIS, Assadin puolustus, Yhdysvaltojen osallistumisen vastustus
- Luottamus mediaan[116]

Listaa tarkastelemalla voidaan tunnistaa selkeä yhteys valintojen välillä. IRA pyrki pelaamaan samanaikaisesti eri puolilla olevia sosiaalisia ryhmiä sekä ruokkimaan näiden välistä vihaa sekä ryhmien kahtiajakoa. Polarisaation ja yhteiskunnan kahtiajaon tavoitteleminen vihan, erimielisyyksien esiin nostamisen sekä kiistakohtien korostamisen kautta oli voimakas osa IRA:n viestintää sen operaation. Monet sen julkaisuista pyrkivät alleviivaamaan toisen puolen argumenttia, tekemään siitä vähemmän uskottavaa ja voimistamaan oikeassa olemisen sekä oikeanmukaisuuden tunteita ryhmien sisällä.

Useissa tapauksissa IRA ei myöskään pyrkinyt luomaan uusia ongelmia tai teemoja, vaan tarttui jo olemassa oleviin jakolinjoihin, sekä ruokki ja voimisti näihin liittyviä tunteita. Tämä osoittaa myös IRA:n syvällistä tuntemusta Yhdysvaltojen sosiaalisista ongelmista ja sekä kehittyneitä kompetensseja sosiaalisen median käyttämisestä.

Kuva 2: Angry Eagle-meemi

Julkaistu IRA:n Angry Eagle-sivulla. Päivämäärää tai tarkkoja tietoja julkaisulle ei annettu. [117]

[116]Aiheet ja teemat: DiRestra, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. 2020. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge.
[117] Ibid.

Yläpuolella oleva IRA:n julkaisema kuva on kohdistettu poliittisesti oikealle nojaavalle, voimakkaasti konservatiiviselle yleisölle. Viestin tarkoituksena on pitkälti heikentää tyypillisesti vasemmistolaisempiin ja liberaalimpiin näkökulmiin liitettyjä argumentteja. Samalla sen tarkoituksena on voimistaa yhteisön tunnetta sen oikeutuksesta ja invalitoida vastustavien argumenttien näkökohtaa ja yleisöä.

Kuva 3: Secure borders-meemi

"As I've said before, I'm really concerned if victory will go to Hillary Clinton due to voter fraud. If we can't trust the State Department, if we can't trust DOJ, if we can't trust the FBI, if we can't trust the DHS, hell we can't trust any division of our Federal Government, so it seems logical we can't put much trust in today's elections system. And we see that Hillary is exhibiting the same cockiness that Obama did before he won in 2008/2012. As if she knows in advance that the results will put her in the White House. POTUS administration shamelessly exploit the rigged system, Democrats already have a great experience at this. Illegal aliens, dead people, incarcerated criminals or refugees who can't even speak English... They ALL work together to get Democrats over the top in these elections!! Are you outraged by this as much as I am? No wonder they trying to take away our guns - because Americans have had enough of this BS and if Killary wins there will be riots nationwide, not seen since the times of Revolutionary war!!" – posted on Secured Borders, 10/7/2016

Julkaistu Secure Borders Facebook sivulla heinäkuussa 2016. [118]

Kuva 2 hyökkää pitkälti Clintonia ja Obamaa vastaan, nostaen IRA:lle tyypillisiä väitteitä vaalihuijauksesta, ääntenlaskentapetoksista sekä muista sen usein esittämistä väitteistä. Julkaisun on tarkoitus herättää vihaa sekä demonisoida toista puolta, syventää kahtiajakoa luomalla viholliskuvia, mutta myös voimistaa sisäryhmän oikeutusta sekä kokemusta oikeassa olemisesta.

IRA on pyrkinyt toimintansa aikana ja operaatioidensa kautta hyökkäämään yhdysvaltalaista yhteiskuntaa kohtaan. Useat sen operaatiot menivät kuitenkin hyvin syvälle, rakentaen ympärilleen useita toisiaan tukevia sosiaalisen median sivuja, verkkosivuja, kauppoja, tuotteita ja brändejä.

Esimerkkinä tästä toiminnasta voidaan tarkastella Black Matters US:n tapausta, joka oli IRA:n hallinnoima sivusto. Tapaus edustaa keskikokoista projektia IRA:lta eikä ollut sen

[118] Ibid.

suurimpia tai menestyneimpiä sivustoja, mutta kuvaa hyvin, miten se kohdensi resursseja afroamerikkalaisiin ja tummaihoisiin kulttuureihin. Se myös näyttää miten taitavasti IRA sovelsi sosiaalisen median eri aspekteja tavoitteidensa saavuttamiseksi.

3.1.6. Black Matters US

Black Matters US on ensimerkki IRA:n monialustaisista astroturffaus-operaatioista. (Astroturffauksesta tarkemmin luvussa 4.5.) Black Matters US:llä oli aktiivisuutta Twitterissä, Facebookissa, Instagramissa, Youtubessa, Google+:ssa, Tumblerissa, sen omalla Blackmatters.us verkkosivulla, sekä Paypalissa, jota se käytti lahjoitusten keräämiseen ryhmälle. IRA hyödynsi tyypillisesti kaikkia näitä tilejä yhtenäisesti, nostaakseen näkyvyyttä tililleen sekä sen julkaisuille sekä tavoittaakseen laajempia yleisöjä. Esimerkiksi Black Matters US:n Twitter sivu julkaisi uutisia sen nettisivulta, sekä julkisti Black Matters US Facebook sivun tapahtumia pyrkien hyödyntämään läsnäoloaan useilla alustoilla saadakseen ihmisiä osallistumaan erilaisiin protesteihin ja kokoontumisiin.[119]

Black Matters US keskittyi sisällössään näennäisesti yhteisön rakennukseen voimistamalla tummaihoista identiteettiä sekä keskittymällä julkaisemaan sisältöjä, jotka vahvistivat tätä kokemusta.

Black Matters US on myös muilla tavoin mielenkiintoinen tapausesimerkki IRA:n toiminnan laajuudesta sekä operaation koossa. Sen monialustainen läsnäolo verkossa kertoi laajasta ja kohdistetusta vaikutuskampanjasta sekä hyvästä käsityksestä verkon ja sosiaalisen median toimintaympäristöstä. Monialustainen läsnäolo antoi sen ohjata liikettä kätevästi verkkosivuilleen, jotka se perusti ensimmäisen Facebook-sivunsa tultua suljetuksi elokuussa 2016 (johtuen sen jakamasta liiallisen kyseenalaisesta ja jakavasta sisällöstä).[120]

Sen Instagram-tilit antoivat sen hioa sekä voimistaa tummaihoisen identiteetin nostamiseen kohdistettua sisältöä, ja Twitter mahdollisti sille tapahtumistaan viestimisen ja verkkosivujensa kautta toimivan meet-up toiminnon mainostamisen, jonka kautta se

[119] Howard, P., Ganesh, B., Dimitra, L., Kelly, J.& Francois, C., 2018. *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* Computational Propaganda Research Project
[120] Ibid.

pystyi organisoimaan protesteja ja muita tapahtumia. Samalla se hyödynsi Youtube-videoita sekä Soundcloud-podcasteja brändin luomiseen sekä kokonaisvaltaisemman yleisön tavoittamiseen. Se hyödynsi myös Redditin ja Pinterestin kaltaisia sivustoja tavoittaakseen uusia yleisöjä ja kasvattaakseen seuraajakuntaansa. Useat sen julkaisuista tavoittivat myös sosiaalisen median vaikuttajia,[121] jotka jakoivat ne uudelleen omille seuraajilleen ja kasvattivat näin Black Matters US:n julkaisujen tavoittavuutta ja yleisön kokoa.[122]

Black Matters US oli myös kekseliäs siinä, miten se tuotti sisältöä ja pyrki vaikuttamaan autenttisemmalta. Se julkaisu useita sisältöjä, joiden tarkoitus oli rekrytoida protestoijia, sisällöntuottajia tai kirjoittajia, aktivisteja, asianajajia sekä valokuvaajia lukuisiin sen järjestämiin protesteihin ja tapahtumiin. Se julkaisi työpaikkailmoituksia yhdysvaltalaisille kirjoittajille palkatakseen heidät tuottamaan sisältöä blackmattersus.com-sivulle. Eri sosiaalisten mediatiliensä kautta se rekrytoi ’designereita’, maahanmuuttoon erikoistuneita asianajajia, pyysi seuraajiaan lähettämään kuvia afroamerikkalaisista naisista kalenterin luomista varten. Se myös etsi osallistujia työn alla olevaan tositv-ohjelmaan pyytäen osallistujia lähettämään lyhyen videon, jolla osallistujien piti kuvata päivittäisessä elämässä kohtaamiaan ongelmia.[123]

Black Matters US sivustojen ja tilien kokonaista kattavuutta yksinään on vaikea arvioida. Blackmattersus.com sivusto ilmoitti, että se oli saavuttanut yli 100 000 seuraajaa. Sen Instagram-tilillä oli yli 25 000 seuraajaa ja sen julkaisut keräsivät noin 2 miljoonaa ”impressiota” olemassaoloaikanaan. IRA mainosti Blackmattersus.com sivustoa sekä Facebookin että Google Adwordsin kautta, käyttäen useita tuhansia mainoksiin. Huolimatta siitä, että se ei ollut IRA:n suurimpia sivustoja tai operaatioita asettuen noin keskipaikoille verrattuna sen muihin brändeihin, sen kattavuus kokonaisuutena oli kuitenkin merkittävä ja tavoitti elinaikanaan luultavasti useita miljoonia käyttäjiä.

[121] Termi ’Influencer’ tarkoittaa henkilöä, jolla on yli 100 000 seuraajan yleisö sosiaalisessa mediassa. Huom. suomeksi 'vaikuttaja'
[122] DiRestra, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. 2020. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge.
[123] Ibid.

Samalla Black Matters US oli vain yksi noin kolmestakymmenestä IRA:n operoimasta Facebook-sivusta, joka kohdisti toimintansa erityisesti afroamerikkalaisiin yhteisöihin.[124]

3.1.7. Toimijoiden kehitys

Black Matters US:n tapauksessa on myös joitakin toimintamalleja, jotka muistuttavat IRA:n toimia sen ylläpitämän Army of Jesus-Facebook sivun yhteydessä. IRA:n rekrytointi ja 'toimijoiden kehitys'[125] vuosien aikana oli hyvin laajamittaista. Sen lukuisten hakuilmoitusten lisäksi (jotka, kuten Black Matters US:n tapauksen kanssa, etsivät ihmisiä joko tuottamaan tekstiä tai sisältöä, etsivät protestoijia, vapaaehtoisia järjestämään erilaisia tapahtumia, valokuvaajia, puhujia tapahtumiin, 'designereita' ja videotuottajia), se myös loi ja mainosti apulinjoja ihmisille, jotka kamppailivat erilaisten seksuaalisten ongelmien/riippuvuuksien kanssa.

IRA:n tarkoitus näiden eri kanavien kanssa oli hyödyntää pitkäaikaista vakoilu- ja tiedustelupiireistä tunnettua menetelmää, jossa toimija käyttää hyväksi henkilökohtaista haavoittuvaisuutta, esimerkiksi salaisuutta tai identiteettiä. Hyödyntämällä tätä haavoittuvaisuutta, henkilö muutetaan manipulaation ja/tai kiristyksen kautta toimijaksi, hänen tosin mahdollisesti tätä tietämättä. Haavoittuvaisuus voi tyypillisesti olla esimerkiksi salaisuus, joka aiheuttaisi häpeää tai taloudellista tai henkilökohtaista harmia tullessaan paljastetuksi.[126] Jatkotutkimukset[127] sekä Yhdysvaltain oikeusministeriön oikeustutkinta[128] osoittavat, että useat ihmiset vastasivat IRA:n ilmoituksiin ja että ne tavoittivat merkittävän määrän ihmisiä. Datasetin rajattu luonne kuitenkin tarkoittaa, että ihmisten tarkkaa määrää on mahdoton arvioida. Selkeämpi käsitys ilmiön kattavuudesta vaatisi jatkotutkimuksia aiheeseen ja uhreihin.

---

[124] DiRestra, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. 2020. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge., https://euobserver.com/eu-china/148618

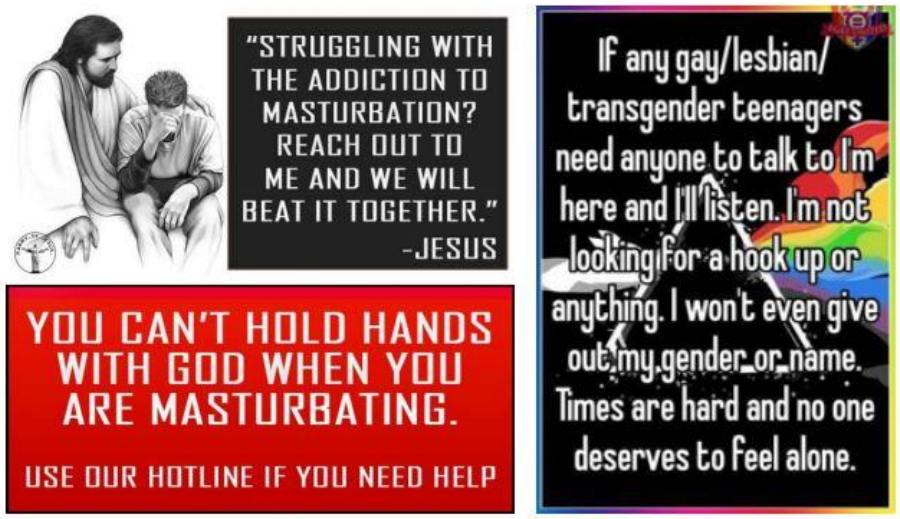
[125] Julkaisut käyttävät termiä "Asset Development", joka on käännetty tässä termiksi toimijoiden kehitys.

[126] DiRestra, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. 2020. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge.

[127] Ibid.

[128] United States District Court for the District of Columbia. 2018. *Indictment: United States of America v. Internet Research Agency LLC, A/K/A Mediasintez LLC A/K/A Glavset LLC A/K/A Mixinfo LLC A/K/A Azimut LLC A/K/A Novinfo LLC, Concord Management and Consulting LLC, Concord Catering, Yevgeniy Viktorovich Prigozhin, Mihkail Ivanocivh Byrstrov, Mikhail Leonidovich Burchik A/K/A Mikhail Abramov, Aleksandra Yuryevna Krylova, Anna Vladislavovna Bogacheva, Sergey Pavlovich Polozov, Maria Anatolyevna Bovda A/K/A Maria Anatolyevna Belyeava, Robert Sergeyevich Bovda, Dzheykhun Nasimi Ogly Aslanov A/K/A Jayhoon Aslanov A/K/A Jay Aslanov, Vladim Vladimirovich Podkopaev, Gleb Igorevich Vasilchenko, Irina Viktorovna Kaverzina, and Vladimir Venkov*. U.S. Justice Department.

Kuva 3:



Vasemmalla oleva kuva julkaistu Facebookissa maaliskuussa 2017, sivulla Army of Jesus. Oikeanpuoleinen kuva julkaistu Instagramissa huhtikuussa 2017, sivulla LGBT United.[129]

On mahdollista, että osa Black Matters US-sivun julkaisuista pyrki toisintamaan sen aiempia yrityksiä kerätä sosiaalisen median käyttäjien henkilökohtaisia tietoja saamalla yksilöt vapaaehtoisesti paljastamaan omia heikkouksiaan.[130] On todennäköistä, että IRA sai käsiinsä materiaalia, joka antoi sen manipuloida tai kiristää ihmisiä (Katso luku 4.7 joka kuvaa tarkemmin kriittisen tiedon käyttämistä yksilöiden tai organisaatioiden kiristämiseksi tai vahingoittamiseksi). Tietoa siitä miten hyvin IRA:n yritykset onnistuivat, ei kuitenkaan ole.

3.1.8. Yhteenveto

IRA operoi monivuotista, yhä käynnissä olevaa disinformaatio- ja vaikutuskampanjaa Yhdysvaltoja vastaan. Kampanjan tarkoituksena oli epävakauttaa yhdysvaltalaista yhteiskuntaa, syventää sosiaalisia kahtiajakoja, ajaa poliittisen keskustelun sekä yhteiskunnan polarisoitumista ja vaikuttaa sen vaaleihin. Monivuotisen kampanjan valmistelu alkoi 2010-luvun alkuvuosina ja se hyödynsi laajalti kompetensseja, joita Venäjä ja IRA olivat kehittäneet aiemmissa kampanjoissaan muun muassa Vietnamin, Ukrainan sekä sen omien kansalaisten manipuloinnissa. IRA:n vaikutuskampanja on

[129] DiRestra, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J. & Johnson, B. 2020. *The Tactics & Tropes of the Internet Research Agency*. New Knowledge.
[130] Ibid.

tavoittanut kymmeniä miljoonia yhdysvaltalaisia ja sen julkaisut ovat keränneet satoja miljoonia ”interkatioita”. On vaikea arvioida, onko kaikki sen operoimista sivuista tunnistettu. Tämän arvioiminen vaatisi sosiaalisen median alustoilta merkittävästi suurempaa läpinäkyvyyttä ja yhteistyötä tutkijoiden sekä viranomaisten kanssa.

IRA:n operaatio itsessään oli poikkeuksellisen laaja ja hyödynsi monialustaisia kokonaisuuksia, jotka myös tukivat ja uudelleen twiittasivat ja mainostivat toisiaan. Useat IRA:n verkossa suoritetuista toimista onnistuivat myös laukaisemaan tapahtumia verkon ulkopuolella johtaen protesteihin, mielenosoituksiin sekä erilaisiin tukitapahtumiin, joita IRA joko järjesti tai johon se etsi osallistujia. Se rekrytoi laajasti sekä vapaaehtoisia että palkattuja henkilöitä tuottamaan sisältöä, toimimaan erilaisissa tehtävissä ja muuten tukemaan toimiaan johtaen henkilöt uskomaan, että he työskentelivät erilaisten sosiaalisten ongelmien parissa. IRA myös pyrki keräämään henkilökohtaista tietoa yksilöistä, joita se myöhemmin olisi voinut käyttää näiden kiristämiseen tai manipulointiin. Vaikuttavaa IRA:n operaatioissa on että se onnistui organisoimaan hyvin oikean maailman tapahtumia Yhdysvalloissa ilman yhdenkään IRA:n toimihenkilön fyysistä läsnäoloa maassa.

IRA kohdensi operaatiotaan merkittävissä määrin afroamerikkalaisiin, jotka olivat eräs IRA:n merkittävimmistä kohderyhmistä. Sen viestintä oli suunnattu sekä vasemmalle että oikealle nojaaviin ryhmiin, pelaten taitavasti molempia puolia argumenteista ja lietsoen ryhmien välistä vihaa, epäluuloisuutta ja kahtiajakoja. Viestiessään presidenttiehdokkaista, IRA:n viestintä Donald Trumpista oli suurimmaksi osaksi positiivista, kun taas Clintonin kohdalla se oli tyypillisesti hyvin negatiivissävytteistä. Viestintä tuki Trumpia myös kritisoimalla tai muuten esittämällä hänen kilpakumppaninsa republikaanisesta puolueesta negatiivisessa valossa. Clintonin kohdalla julkaisut viestivät positiiviseen sävyyn hänen kilpakumppaneistaan, erityisesti Bernie Sandersista ja Jill Steinistä. Tästä voidaan päätellä, että on selkeää, ettei Venäjä halunnut Clintonin voittavan presidentinvaaleja, kun se taas näki Trumpin omille tavoitteilleen erittäin sopivana ehdokkaana.

Operaatioita voidaan nähdä jatkeena Venäjän pitkäaikaiselle vihamielisyydelle ja kilpakumppaniudelle Yhdysvaltoja kohtaan. Perinteisen sodankäynnin keinojen Venäjä on siirtynyt epäsuoraan, asymmetriseen informaatiosodankäyntiin, jossa se voi

epäsuorasti vaikuttaa haastajiinsa mutta samalla toimia perinteisen sodankäynnin tai suoran konfliktin kynnyksen alapuolella.

On myös epäselkeää, miten Yhdysvallat tulee vastaamaan Venäjän ja informaatiosodankäyntiin sitä kohtaan. Tämänhetkisen presidentin hyötyessä Venäjän operaatioista, on mahdollista, että merkittävää vastausta ei tulla näkemään ja Venäjä saa jatkaa toimiaan pitkälti ilman seurauksia. Toisaalta mikäli Trump häviää presidentinvaalit marraskuussa 2020, on todennäköistä, että Yhdysvaltojen ulkopolitiikka tulisi heijastamaan merkittäviä muutoksia, jotka saattaisivat johtaa myös avoimempiin vastauksiin Venäjän toimia vastaan. Keskeisenä haasteena vastaukselle voisi kuitenkin olla vakuuttaa kansainvälinen yhteisö siitä, että Yhdysvalloilla on riittävä oikeus sanktioihin tai muuhun vastaukseen. Toisaalta mikä tahansa aseellinen vastaus tulkittaisiin todennäköisesti suhteettomaksi toimeksi, joka johtaisi jännitteiden merkittävään kasvuun. Tässä suhteessa ei kuitenkaan ole olemassa selkeää ennakkotapausta, sillä maiden välinen välien selvittely informaatiosodankäynnin tai disinformaatiokampanjoiden seurauksena tällä tavalla on jotain mille maailmanhistoria ei tarjoa suoraa rinnakkaiskohtaa tai aiempaa esimerkkiä.

3.2. COVID-19 pandemia ja disinformaatio

Vuoden 2019 lopussa Wuhanissa, Kiinassa tunnistettiin uusi tartuntatauti, Covid-19 tai koronavirustauti. Viruksen leviäminen alkuvuodesta 2020 johti WHO:n julistamaan taudin olevan kansainväliseksi terveysuhaksi tammikuussa 2020.[131] Myöhemmin, maaliskuussa 2020, WHO julisti tilanteen pandemiaksi taudin leviämisen jatkuessa ja infektiotilanteen pahentuessa.[132]

Koronaviruksen aiheuttama pandemia on johtanut merkittäviin taloudellisiin ja sosiaalisiin muutoksiin. Pandemian aiheuttamat liikkumis-, aukiolo- ja kokoontumisrajoitukset ovat johtaneet sekä yritysten, ravintoloiden ja kauppojen sulkeutumisiin, oppilaitosten ja työpaikkojen etätyöskentelyyn ja -opetukseen sekä valtavaan määrään mis- ja disinformaatiota sosiaalisessa mediassa. Tyypilliset disinformaation muodot ovat vaihdelleet salaliittoteorioista (Koronavirus on bioase)

[131] WHO. 2020. *Statement on the second meeting of the International Health Regulations (2005) Emergency Committee regarding the outbreak of novel coronavirus (2019-nCov).* Statement.
[132] WHO Director-General Tedros Adhanom Ghebreyesus. 2020. *WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020.* WHO. Speech

haitallisiin tai suoranaisesti vaarallisiin hoito ohjeisiin (valkaisuaineen piikittäminen tappaa koronavirusta) ja poliittiseen tai geopoliittiseen propagandaan (koronavirus on yhdysvaltalaisten terveysyritysten luoma virus lääkkeiden ja rokotteiden myymiseksi.)[133]

Osa tapauksista on kaupallisesti motivoitunutta, pelosta ja epäluuloista hyötyvää toimintaa, kuten esimerkiksi valkaisuainetta ihmelääkkeenä verkossa myyvät sivustot.[134] Pieni osa on luultavasti myös aidosti erilaisiin salaliittoteorioihin uskovien aloittamaa, yhtä lailla pelon motivoimaa misinformaatiota. On kuitenkin selkeää, että merkittävä osa disinformaatiosta koostuu(tosin huomaten että mis- ja disinformaation raja muuttuu määritelmällisesti hankalaksi joissakin tapauksissa) eri valtiollisten toimijoiden, kuten Kiinan ja Venäjän, järjestelmällisesti levittämästä propagandasta, jonka tarkoitus on palvella näiden maiden poliittisia tavoitteita.[135] Itseasiassa valtiollisten toimijoiden, kuten Kiinan ja Venäjän aktiivisuus disinformaation levittämisessä koronaviruksesta (sekä muista aiheista) on hyvin dokumentoitua ja selkeää. Suurin vastaamaton kysymys onkin se, kuinka suuresta osasta koronaviruksesta liikkuvasta mis- ja disinformaatiosta nämä toimijat tarkalleen ovat vastuussa.

Osio keskittyy erityisesti tarkastelemaan valtiollisten toimijoiden levittämää disinformaatiota koronavirus-pandemian yhteydessä. Keskeisimmät tunnistetut valtiolliset toimijat, jotka ovat levittäneet disinformaatiota koronaviruksesta ovat Kiina ja Venäjä.[136] Tutkijat ovat kuitenkin havainneet koordinoituja vaikutusyrityksiä, jotka ovat keskittyneet muun muassa Turkkiin, Iraniin, Paraguayhin ja Saudi-Arabiaan.[137] Näissä maissa laajat valtiolliset vaikutusverkot pyrkivät hyödyntämään laskennallisen propagandan mahdollisuuksia disinformaation levittämiseksi.

---

[133] EEAS. 2020. *EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the Covid-19 Pandemic. (Update 23 April – 18 May).* https://www.bbc.com/news/world-us-canada-52407177, https://www.washingtonpost.com/nation/2020/07/09/fake-coronavirus-cure-bleach/

[134] https://www.theguardian.com/world/2020/sep/19/bleach-miracle-cure-amazon-covid

[135] EEAS. 2020. *EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the Covid-19 Pandemic. (Update 23 April – 18 May).*

[136] EEAS. 2020. *EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the Covid-19 Pandemic. (Update 23 April – 18 May)*., https://euobserver.com/eu-china/148618

[137] Graham, T., Bruns, A., Zhu, Guangnan & Campbell, R. 2020. *Like a Virus: The Coordinated Spread of Coronavirus Disinformation.* Centre for Responsible Technology & The Australia Institute., Rebello, K., Schwieter, C., Schliebs, M., Joynes-Burgess, K., Elswah, M., Bright, J. & Howard, P. 2020. Covid-19 News and Information from State-Backed Outlets Targeting French, German and Spanish-Speaking Social Media Users. COMPROP Data Memo 2020.4

Useissa tapauksissa disinformaatiota pyritään levittämään juuri astroturffauksen ja bottiverkkojen kautta hyödyntäen laajoja koordinoituja verkostoja autenttisen näköisten ilmiöiden luomiseksi. Myös valtiolliset toimijat ovat viimeisten vuosien aikana kehittäneet merkittävää osaamista näiden keinojen soveltamisesta. (Katso boteista ja bottiverkoista lisää luvusta 4.1 ja astroturffauksesta luvusta 4.6)

3.2.1. Venäjä

Venäjällä on merkittävä historia disinformaation, vaikuttamisen, manipulaation sekä propagandan tuottajana, kohdistaen sitä sekä länsimaihin että omiin kansalaisiinsa.[138] Kreml-myönteiset lähteet levittävät aktiivisesti koronavirukseen liittyvää disinformaatiota ja pyrkivät voimistaman (amplifioimaan) olemassa olevia salaliittoteorioita sekä levittämään uusia. (Katso amplifikaatiosta lisää luvusta 4.2.) Näistä tyypillisiä esimerkkejä ovat olleet Koronavirus-pandemian linkittäminen bioaseeseen ja biologiseen sodankäyntiin. Toimijat ovat myös levittäneet teoriaa siitä, että 5G-verkot ja 5G-tukitornit levittävät koronavirusta. Yhtäläisesti osa viesteistä on keskittynyt rokotevastaisuuteen sekä rokotteiden turvallisuuden kyseenalaistamiseen.[139]

Venäjän keskeisimmät kohteet koronaviruspandemian aikana ovat olleet länsimaat, EU, Nato ja Yhdysvallat. Toisaalta Venäjä on alkanut kohdistaa disinformaatiota myös esimerkiksi Bill ja Melinda Gatesia sekä Gates Foundationia kohtaan.[140] EEAS projekti, EUvsDisinfo on kerännyt tähän mennessä (Elokuu 2020) noin 600 esimerkkiä venäläislähtöisesti koronavirukseen liittyvästä disinformaatiosta.[141] Tietopankki esittää laajan ja melko selkeän sekä yhtenäisen kuvan venäläislähtöisestä disinformaatiosta.

---

[138] EEAS. 2020. *EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the Covid-19 Pandemic. (Update 23 April – 18 May).*
[139] Ibid.
[140] Mm. https://euvsdisinfo.eu/report/us-protests-organised-by-bill-gates/., https://euvsdisinfo.eu/report/bill-gates-pays-compensations-to-people-mutilated-as-a-result-of-the-vaccines/., https://euvsdisinfo.eu/report/bill-gates-wants-to-use-vaccines-to-cull-humanity/., https://euvsdisinfo.eu/report/coronavirus-in-italy-striped-down-european-unity/., https://euvsdisinfo.eu/report/nato-is-an-aggressive-coronavirus-of-capitalism-us-and-ukrainian-fascists-are-in-war-against-russia/., https://euvsdisinfo.eu/report/the-coronavirus-was-engineered-in-france-and-a/., https://euvsdisinfo.eu/report/coronavirus-proved-that-nato-is-pointless/., https://euvsdisinfo.eu/report/nato-pays-belarusian-opposition-1-per-one-person-infected-with-coronavirus/.
[141] https://euvsdisinfo.eu/disinformation-cases/?disinfo_keywords%5B%5D=106935&date=&per_page=100

Venäjä hyödyntää tehokkaasti bottiverkkojen, amplifikaation, astroturffauksen ja valeuutisten keinoja levittääkseen disinformaatiota. (Katso luvut 4.1, 4.2, 4.4 ja 4.6). Laaja osa disinformaatiosta on suoraan lähtöisin valtio-omisteisista medioista. Tuottamalla uutisia esimerkiksi Sputnik tai RT:n maakohtaisten sivustojen kautta ja käyttämällä bottiverkostoja levittämään näitä sosiaalisessa mediassa sekä saaden astroturffauksen kautta sen näyttämään aidolta ilmiöltä, Venäjä on onnistunut hyvin tehokkaasti levittämään viestejään sosiaalisen median kautta myös lännessä. Oxfordin julkaisemassa tutkimuksessa tutkijat havaitsivat valtiolähtöisten disinformaatioviestien saavuttavan korkeampia jako- ja reaktiomääriä kuin useat tunnetut ja luotettavammat uutislähteet.[142] Venäläislähtöinen disinformaatio onnistui noin kahden viikon aikaväillä (18. toukokuuta – 5. kesäkuuta) tavoittamaan noin 1.2 miljoonaa ihmistä Ranskassa, 350 000 ihmistä Saksassa ja noin 4 miljoonaa ihmistä Espanjassa.[143]

Tutkimuksen mukaan Venäjän viestien sisältö näissä maissa keskittyi pääasiassa kahteen. Näistä ensimmäinen, heikot demokratiat ja instituutiot, keskittyi korostamaan protesteja ja siviilitottelemattomuutta sekä kiristyneitä suhteita julkisiin viranomaisiin pandemian aikana. RT Ranska ja RT Tanska molemmat jakoivat uutisia, kuvia ja videoleikkeitä terveydenhuollon työntekijöiden Belgian pääministeriä vastaan järjestämästä hiljaisesta protestista, jossa osallistujat ”käänsivät selkänsä” pääministerille tämän vieraillessa sairaalassa, jossa protesti järjestettiin. Toinen Sputnik Ranskan kirjoittama artikkeli esitti, että koronavirus-rajoitukset sekä siitä seuraava talouskriisi voisivat johtaa kansannousuun Ranskassa. Toinen tutkijoiden havaitsema aihe käsitteli erityisesti salaliittoteorioita. Mielenkiintoisena uutena esimerkkinä nostetaan Venäjän käyttämä strategia, jossa RT Tanska uutisoi italialaisen poliitikon vaatineen Bill Gatesia pidätettäväksi rikoksista ihmiskuntaa vastaan. Artikkelissa RT Tanska pilkkaa väitöksiä ”absurdeina”, mutta tästä huolimatta uutisoi niistä merkittävällä tarkkuudella ja yksityiskohtaisuudella, nostaen esille väitteitä siitä, miten Gates Foundation yrittää ajaa läpi lakimuutosta pakkorokotuksista sekä miten sen aiemmat rokotuskampanjat sterilisoivat miljoonia naisia Afrikassa.[144]

---

[142] Rebello, K., Schwieter, C., Schliebs, M., Joynes-Burgess, K., Elswah, M., Bright, J. & Howard, P. 2020. *Covid-19 News and Information from State-Backed Outlets Targeting French, German and Spanish-Speaking Social Media Users.* COMPROP Data Memo 2020.4., Bright, J., Au, H., Bailey, H., Elswah, M., Schliebs, M., Marchal, N., Schwieter, C., Rebello, K., Howard, P., *Coronavirus Coverage by State-Backed English-Language News Sources.* COMPROP Data Memo 2020.2

[143] Ibid.

[144] Ibid.

Venäjä vaikuttaa luottavan pitkälti perinteisempiin ja selkeämmin muodostettuihin väyliin koronavirukseen liittyvän disinformaation levittämisessä. Se käyttää erityisesti kohdennetuilla kielillä sisältöä tuottavia, maakohtaisempia julkaisujaan, kuten RT:tä ja Sputnikia, tuottamaan valeuutisia ja disinformaatiota, jolla se voi tavoittaa merkittäviä yleisöjä.

Kuva Venäjän levittämästä koronavirus-disinformaatiosta poikkeaa jossain määrin sen toimista esimerkiksi Yhdysvalloissa luvussa 4.1. Tätä eroa voi selittää esimerkiksi se, että sillä ei ole samankaltaista valmista lukijakuntaa ja yleisöjä Yhdysvalloissa sen julkaisuille tai että se ei koe voivansa saavuttaa tällaista esimerkiksi heikon maakuvan tai ennakkoluulojen takia. Toisaalta eroa voi myös selittää ilmiön tuoreus. On mahdollista, että Venäjä käyttää sisältöjen levittämiseen samanlaisia mekanismeja (laajamittaista astroturffausta, sosiaalisen median manipulointia, koordinoitua amplifikaatiota), mutta koska ilmiö itsessään on elää yhä, näitä toimia ei ole vielä ehditty havaita tai tutkijat ja turvallisuusyhteisöt Euroopassa eivät ole ehtineet reagoida niihin.

Toisena ongelmana on myös disinformaatiokampanjoiden vastuun tarkempi kohdistaminen yksittäisille toimijoille. Carnegie Mellon-yliopiston tutkijat havaitsivat toukokuussa, että suurin osa Yhdysvalloissa käytävästä keskustelusta yhteiskunnan jälleen avaamisesta oli bottien ajamaa. Tutkijoiden analysoimasta 200 miljoonasta twiiteistä, 66 % kaikista twiiteistä oli todennäköisestä automatisaation avustuksella tuotettuja, ja 34 % kaikista twiiteistä olivat varmasti bottien tuottamia. Samalla tutkijat havaitsivat, että 50 eniten levikkiä saavista uudelleentwiittaajista 82 % olivat botteja ja 1000 eniten levikkiä saavasta uudelleentwiittaajasta vastaava luku oli 62 %.[145] Vaikka tutkimuksen tulokset osoittavat selvästi laajamittaisen disinformaatiokampanjan aiheesta olevan käynnissä, myös tutkijat itse toteavat, että vaikka ”operaatio näyttää propaganda-koneelta ja se vastaa selkeästi Venäjän ja Kiinan aiempia toimitapoja ja menetelmiä, vaatisi valtavan määrän resursseja vahvistaa tämä epäily”.[146] Toisin sanoen siis vaikka voimme selkeästi havaita disinformaatiokampanjan olevan käynnissä, merkittäväksi

[145] https://www.scs.cmu.edu/news/nearly-half-twitter-accounts-discussing-reopening-america-may-be-bots
[146] Ibid.

ongelmaksi muodostuu se, ettei siitä vastuun kohdistaminen yksittäisille toimijoille tai näiden toimijoiden nimeäminen, useimmissa tapauksissa ole vielä mahdollista.

On myös mahdollista, että sen toimien ainakin osittain tultua valoon Yhdysvalloissa ja Iso-Britanniassa, Venäjä on osaltaan muuttanut toimintastrategiaansa tai kehittänyt vaikeammin havaittavia keinoja ja parantanut kompetenssejaan sosiaalisen median manipulaatiossa. Onkin todennäköistä, että tulee viemään useita vuosia ennen kuin ilmiöstä voidaan muodostaa selkeä kokonaiskuva.

Venäjän toimien ja sen levittämän disinformaation kattavuutta on vaikea arvioida tarkasti. Merkittävimpänä kysymyksenä ei olekaan ”osallistuuko Venäjä aktiivisesti disinformaation levittämiseen koti- tai länsimaissa”, tai ”käyttääkö Venäjä sosiaalista mediaa disinformaation levittämiseen” vaan ”kuinka laajasti Venäjän toimet vaikuttavat yhteiskuntien kykyyn vastata koronaviruspandemiaan”. Kysymykseen vastaaminen on tämän työn laajuuden ulkopuolella, mutta esittää hyvin tärkeää tutkimussuuntaa jatkotutkimukselle. Valitettavasti tämä vaatisi kuitenkin pääsyä Facebookin, Twitterin ja Googlen tietokantoihin, joka toistaiseksi näyttää jossain määrin epätodennäköiseltä.

On siis selvää, että Venäjä pyrkii aktiivisesti heikentämään länsimaisia yhteiskuntia levittämällä disinformaatiota sekä samalla ajamaan ja edustamaan omia poliittisia tavoitteitaan ulkomailla. Huolestuttavaa itseasiassa onkin, että tarkastelemalla sekä uutisten herättämiä reaktioita sekä jakoja sosiaalisessa mediassa voidaan myös huomata, että venäläislähtöiset valeuutiset ovat usein levinneet laajemmalle kuin itsenäisten ja arvostettujen uutistalojen julkaisut. Tämä vahvistaa käsitystä siitä, että kyseessä on laajempi ongelma kuin aiemmin on tiedostettu.

3.2.2. Kiina

Toinen merkittävä tunnistettu disinformaatiotoimija koronavirus-pandemian aikana on ollut Kiina. Vaikka Venäjän disinformaatio-operaatiot ovat saaneet viimeisten vuosien aikana erityisesti mediassa enemmän näkyvyyttä, Kiinan kokemus disinformaatio-operaatioista on vähintäänkin samaa luokkaa kuin Venäjän ja sen resurssit todennäköisesti merkittävästi suuremmat. Vuonna 2019 julkaistu tutkimus Oxfordin Computational Propaganda Projectilta arvioi Kiinan työllistävän 300 000–2 000 000 ihmistä

organisoituun sosiaalisen median ja internetin manipulointiin.[147] Arviot eivät erottele sen suhteen, kuinka suuri osa näistä henkilöistä työskentelee kotimaisten ja ulkomaisten projektien parissa.[148] On kuitenkin todennäköistä, että Kiinan resurssit ja operaation koko tekevät siitä erään maailman merkittävimmistä toimijoista osa-alueella.

Kiinan toiminta on useimmissa havaituissa tapauksissa muistuttanut pitkälti Venäjän operaatioita toimitavoiltaan. Se käyttää laajasti erilaisia ulkomaille suunnattuja valtiollisia medioitaan, kuten CGTN:n, China Dailya ja Xinhuaa. Kiina tuottaa näiden kautta sisältöjä Kiinan ja Englannin lisäksi myös monilla muilla kielillä, kuten saksaksi, ranskaksi ja italiaksi. Ne keskittyvät temaattisesti osittain samankaltaisiin teemoihin kuin Venäjän tuottama disinformaatio. Jaettu teema on demokraattisten maiden heikko vastaus koronavirukseen ja sen huono hoito sekä kansalaisten tyytymättömyys omiin johtajiinsa, virkamiehiin ja demokraattiseen prosessiin. Tyypillisenä motiivina vaikuttaa olevan tyytymättömyyden nostaminen sekä viranomaisiin kohdistuvan luottamuksen laskeminen kansalaisten keskuudessa.[149]

Toinen keskeinen Kiinan käyttämä teema, joka heijastuu erittäin voimakkaana sen viestinnässä, on kritiikin ohjaaminen pois sen omista toimista. Kiina on pyrkinyt ylistämään omia toimiaan pandemian hoitamisessa sekä luomaan ja vahvistamaan positiivista maakuvaa. Kiinalle on ollut poikkeuksellisen tärkeää esittää, että se on onnistuneesti rajoittanut viruksen leviämistä. Näin se yrittää asettautua esimerkkimaaksi viruksen hoitamisessa.[150] Esimerkkeinä tästä ovat olleet *a People's Dailyn* julkaisema uutinen, joka ylisti akateemikkoja Chinese Academy of Sciences and Chinese Academy of Engineeringistä, jotka ovat tulleet tunnetuiksi ”valkoiseen pukeutuneina sotureina”.[151] *A China Dailyn* artikkeli kuvasi Wuhania ’Paikkana, joka antaa toivoa maailmalle’. Samalla julkaisulla on myös osio verkkosivussaan, joka mainostaa ’Koronavirusta vastaan taistelemista kiinalaisella tavalla’ esittäen erilaisia Kiinan perinteisen lääketieteen parannuskeinoja vastauksena koronavirukseen.[152]

[147] Bradshaw, S. & Howard, P. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*. Computational Propaganda Research Project.
[148] Ibid.
[149] Ibid.
[150] Ibid.
[151] http://en.people.cn/n3/2020/0319/c90000-9669975.html
[152] https://covid-19.chinadaily.com.cn/

Kolmas ja Venäjän kanssa voimakkaasti jaettu teema myös Kiinan kohdalla on ollut salaliittoteorioiden levittäminen ja amplifiointi. (Katso luku 4.2 amplifikaatiosta.) Esimerkiksi CGTN:n lainasi artikkelissaan italialaista tutkijaa, joka kertoi viruksen mahdollisesti kehittyneen Italiassa.[153] Useat Kiinan julkaisuista ovat tukeneet tätä esittämällä raportteja, joiden mukaan Koronavirus ei välttämättä olisi lähtöisin Kiinasta mukaan lukien Kiinan Koronavirus-asiantuntijapaneelin johtaja, Zhong Nanshan. CGTN julkaisi aiheesta pääkirjoituksen, jossa se esitti, että koronavirus olisi voinut tulla Wuhaniin Yhdysvaltain armeijan kantamana.[154]

Vastauksena Kiinan toimiin, muun muassa sosiaalisen median alusta Twitter ilmoitti poistaneensa kesäkuun alussa alustaltaan 175 000 Kiinaan liitettyä käyttäjätiliä. Käyttäjätilit olivat levittäneet disinformaatiota koronaviruksesta ja Hong Kongin protesteista.[155] (Katso luku 4.1 boteista ja bottiverkoista.) Keskeistä olisikin, että Twitter jakaisi tiedot poistetuista käyttäjistä, niiden toimista ja interaktioista muiden käyttäjien kanssa tutkijoille, joka mahdollistaisi erityisesti kiinalaislähtöisen disinformaation analysoimisen ja valottaisi ilmiötä laajemmin myös tältä puolelta.

3.2.3. Yhteenveto

Valtiolliset toimijat kuten Venäjä ja Kiina levittävät aggressiivisesti disinformaatiota, jonka tarkoitus laajasti on vaikuttaa sekä asenteisiin, uskomuksiin että heittää epäilystä oikeisiin terveyskäytäntöihin ja faktatietoon. Toistaiseksi niiden tahti ei vaikuta heikentyneen, eivätkä ne vaikuta kantavan merkittävää huolta toimiensa merkityksestä hinnasta.

Sosiaalisessa mediassa kohdatulla disinformaatiolla on kuitenkin selkeitä vaikutuksia yksilöiden käytökseen todellisessa maailmassa. Cambridgen tutkijat havaitsivat, että sosiaalisen median käyttö ja salaliittoteorioille altistuminen saivat henkilöt osallistumaan koronaviruksen leviämistä hidastaviin ja terveyttä suojaaviin toimenpiteisiin kuten

[153] https://news.cgtn.com/news/2020-03-22/Coronavirus-may-have-existed-in-Italy-since-November-local-researcher-P4i2As2OAg/index.html
[154] https://news.cgtn.com/news/2020-03-19/10-questions-for-the-U-S-Where-did-the-novel-coronavirus-come-from--OZrgRTSZfa/index.html
[155] https://www.cnbc.com/2020/06/12/twitter-takes-down-china-linked-accounts-spreading-disinformation.html

käsienpesuun, maskien käyttöön ja liikkumisrajoituksiin merkittävästi harvemmin.[156] Samalla salaliittoteoriat sosiaalisessa mediassa esimerkiksi 5G:n verkkoyhteyksien ja koronaviruksen linkeistä ovat johtaneet noin 80 5G-tukitornin vandalisointiin ja polttamisiin Iso-Britanniassa. Tämän lisäksi noin 40 teleoperaattoreiden työntekijää on joutunut verbaalisten ja fyysisten hyökkäysten kohteeksi. Pahimmillaan työntekijän on täytynyt jopa hakeutua sairaalahoitoon hyökkäyksen seurauksena saatuaan teräaseella aiheutetun iskuhaavan.[157]

Sekä sosiaalisen median levinneisyys että disinformaation yleisyys sosiaalisessa mediassa pahentavat ongelmaa yhä enemmän. Kaksi kolmasosaa yhdysvaltalaisista kertoi osana kyselytutkimusta nähneensä sosiaalisessa mediassa informaatiota, joka vaikutti ’keksityltä tai järjenvastaiselta’.[158]

Toistaiseksi merkittävimpinä disinformaation lähteinä on tunnistettu pääasiassa Venäjän, Kiinan ja Iranin omistamia tai suoraan tukemia valtiollisia uutistaloja tai medioita, kuten RT, Sputnik, CGTN ja A People’s Daily.

Toistaiseksi tarkkaa tutkimustietoa näiden valtiollisesti sponsoroitujen disinformaatiouutisten leviämisestä koronaviruksen yhteydessä ei ole olemassa. Tämä on kuitenkin hyvin mielenkiintoinen ja tärkeä osa-alue. Olisi hyödyllistä tunnistaa mekanismeja, joita erityisesti Kiina ja Venäjä käyttävät levittääkseen viestejä sosiaalisessa mediassa. On todennäköistä, että ne eivät poikkea merkittävästi niiden aiemmista toimitavoista, mutta tarkempi tutkimus voisi sekä varmistaa asian että ohjata vastatoimia. On myös huomata, että useissa tapauksissa itse käyttäjät ovat yhtä suuressa vastuussa disinformaation levittämisestä (tosin tahattomasti) kuin sitä tarkoituksellisesti levittävät toimijat, sillä käyttäjät itse päätyvät jakamaan ja levittämään näitä uutisia.[159] Tämä kuvastaa hyvin tarvetta parempaan digitaaliseen lukutaitoon kuten myös

---

[156] Allington, D., Duffy, B., Wessely, S., Dhavan, N., & Rubin, J. 2020. Health-protective behaviour, social media usage and conspiracy belief during the COVID-19 public health emergency. *Psychological Medicine,* 1-7.

[157] https://www.theguardian.com/world/video/2020/may/01/why-the-5g-coronavirus-conspiracy-theory-is-false-video-explainer, https://www.cnet.com/health/5g-coronavirus-conspiracy-theory-sees-77-mobile-towers-burned-report-says/

[158] https://www.journalism.org/2020/04/29/about-seven-in-ten-u-s-adults-say-they-need-to-take-breaks-from-covid-19-news/

[159] Graham, T., Bruns, A., Zhu, Guangnan & Campbell, R. 2020. *Like a Virus: The Coordinated Spread of Coronavirus Disinformation.* Centre for Responsible Technology & The Australia Institute

sosiaalisen median alustojen toimiin. Ilman käyttäjiä, jotka eivät ole valmiita uskomaan näiden toimijoiden viesteihin, eivät niiden viestitkään leviä yhtä kattavasti. Näillä toimilla voi olla myös merkittävä rooli nykyisen, kuin myös seuraavan pandemian ehkäisyssä ja kukistamisessa.

3.3. Disinformaation vaikutukset

Disinformaatiolla on aina ollut todellinen hinta. Maailmanlaajuisen pandemian myötä tämä hinta on kuitenkin tullut selkeämmäksi ja sen vaikutukset välittömämmiksi. Koronaviruksen leviämisen torjunta nojaa pitkälti yksilöiden kykyyn seurata suosituksia taudin torjumisesta. Käsienpesu, sosiaalinen etääntyminen ja maskien käyttö ovat olleet keskeisiä askelia viruksen leviämisen hidastamisessa ja pysäyttämisessä. Samalla maat, joissa kansalaisten luottamus valtioon on korkea, ovat selvinneet merkittävästi paremmin koronaviruksesta.[160] Luottamus valtioon ja instituutioihin on tarkoittanut, että näiden maiden kansalaiset seuraavat todennäköisemmin ohjeita turvatoimista koronavirus-pandemian aikana.[161] Maat, joissa luottamus on ollut alhainen sekä vastatoimet hitaita, ovat kärsineet pandemiasta enemmän. Seurauksena on ollut kuolonuhrien suurempi määrä.

Disinformaation vaikutukset iskevät suoraan tähän pisteeseen. Disinformaatio laskee kansalaisten luottamusta valtioon ja instituutioihin ja voi saada ihmiset kyseenalaistamaan oikeita toimia ja ohjeita tartunnalta suojautumiseksi ja pandemian pysäyttämiseksi.[162] Yli kolmasosa englanninkielisestä (39 %) koronavirus-misinformaatiosta sisältää valheellisia väittämiä viranomaisten käyttämistä toimista tai suosittelemista ohjelinjoista.[163] Vaikka on vaikea arvioida, mikä osuus tästä on valtiollisten toimijoiden levittämää disinformaatiota, luvun 3.2 perusteella on todennäköistä, että niillä on merkittävä rooli osana sitä. Samalla esimerkiksi merkittävä osuus (38 %) yhdysvaltalaisista on myöntänyt, että heillä on haasteita erottaa luotettavien

[160] Oksanen, A., Kaakinen, M., Latikka, R., Savolainen, I., Savela, N. & Koivula, A. 2020. Regulation and Trust: 3-Month Follow-up Study on COVID-19 Mortality in 25 European Countries. *JMIR Public Health Surveillance*;6(2):e19218

[161] https://www.tuni.fi/en/news/new-study-finds-social-factors-decisive-fight-against-covid-19

[162] Oksanen, A., Kaakinen, M., Latikka, R., Savolainen, I., Savela, N. & Koivula, A. 2020. Regulation and Trust: 3-Month Follow-up Study on COVID-19 Mortality in 25 European Countries. *JMIR Public Health Surveillance*;6(2):e19218

[163] Howard, P. 2020. The Science and Technology of Lie Machines. Howard. P. *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*. London: Yale University Press.

ja epäluotettavien koronavirus-informaation lähteiden välillä. Tätä havainnollisti myös, että noin kolmasosa niistä kyselyyn vastaajista, jotka olivat kuulleet salaliittoteorian siitä, että koronavirus oli laskettu liikkeelle tahallisesti vallassa olevien ihmisten päätöksen seurauksena, uskoivat teoriaan jossain määrin.[164]

Myös WHO on tunnistanut mis- ja disinformaation merkityksen globaalin pandemian aikana. Vuoden 2020 kesä- ja heinäkuun aikana WHO järjesti ensimmäisen infodemiologian konferenssin. Konferenssin tarkoituksena oli tuoda yhteen eri maiden viranomaisia, sosiaalisen median ammattilaisia sekä eri alojen tutkijoita ymmärtämään, tutkimaan ja tuottamaan ratkaisuja Covid-19 viruksen infodemian. WHO tunnistaa, että infodemia on kasvanut tasolle, joka vaatii koordinoituja vastauksia ja yhteistyötä eri osa-alueiden toimijoilta.[165]

Samalla muun muassa Kiinan ja Venäjän rooli disinformaation ajajina koronaviruksen yhteydessä on ollut merkittävä. Vaikka tällaisen disinformaation vaikutusta tai hintaa ihmishengissä tai julkisissa kustannuksissa kuolemien, sairastumisien ja pandemian pitenemisen kautta on vaikea mitata, on todennäköistä, että sen kokonaiskustannukset tullaan euromääräisesti laskemaan miljardeissa ennemmin kuin miljoonissa.

Disinformaation ollessa sekä laajalle levinnyttä että uskottavaa, sen vaikutus kasvaa merkittävästi. Toistaiseksi disinformaation kustannusta ihmishengissä yhteydessä on mahdotonta arvioida tarkasti. Kuitenkin jo pelkästään huhu siitä, että koronaviruksen voi parantaa nauttimalla alkoholipohjaista desinfiointiainetta, metanolia, on tappanut yli 800 ihmistä, johtanut noin 6000 hakeutumaan sairaalahoitoon ja aiheuttanut 60 ihmiselle täydellisen näönmenetykseen.[166] Samalla tämä ei ole laajimmalle levinnyt tai merkittävin huhu koronavirukseen liittyen, tosin yksilöterveyden tasolla se voi olla yksi vaarallisimmista.

---

[164] Brennen, S., Simon, F., Howard, P. & Nielsen, R., 2020. *Types, Sources and Claims of COVID-19 misinformation.* Mitchell, A., Jurkowitz, M., Oliphant, B. & Shearer, E., 2020. *Three Months in, Many Americans See Exaggeration, Conspiracy Theories and Partisanship in COVID-19 News.* Pew Research Center

[165] WHO. 2020. *1st WHO Infodemiology Conference.* https://www.who.int/teams/risk-communication/infodemic-management/1st-who-infodemiology-conference., WHO. 2020. *1st WHO Infodemiology Conference.* Event. https://www.who.int/news-room/events/detail/2020/06/30/default-calendar/1st-who-infodemiology-conference

[166] Bateman C,. 2007. Paying the price for AIDS denialism. *Southern African Medical Journal*. Vol. 97, No 10.

Nykytilanteeseen jossain määrin rinnastettava esimerkki voi kuitenkin löytyä HIV-epidemian aikaisilta päiviltä. Huhut siitä, ettei HIV-virusta ollut olemassa ja että sen hoito olisi myrkyllinen ihmiselle, johtivat siihen, että useat ihmiset kieltäytyivät hoidosta Etelä-Afrikassa. Tämän lisäksi Etelä-Afrikan valtio myös suositteli perinteisiä hoitokeinoja HIV-virusta vastaan, jotka johtivat sen laajempaan leviämiseen. Yhdessä nämä toimet maksoivat yli 300 000 ihmisen hengen.[167]

Tähän mennessä koronavirus on hiukan yli puolen vuoden aikana vaatinut noin 800 000 ihmisen hengen. Arviot sen kustannuksista maailmantaloudelle vaihtelevat 5–25 biljoonan välillä.[168] Samalla myös sen mukanaan tuomat talouskustannukset tulevat todennäköisesti aiheuttamaan ennenaikaisia kuolemia vaatien kaksinkertaisen kustannuksen ihmishengissä. Disinformaation merkitystä osana esimerkiksi pandemian leviämistä on vaikea arvioida. On kuitenkin selkeää, että se on hyvin vakavaa.

Tämä tarkastelu ei harkitse disinformaation laajempia vaikutuksia, esimerkiksi sen roolia yhteiskunnallisten kahtiajakojen syventämisessä, tai siinä, mitä laajempia seurauksia esimerkiksi institutionaalisen tai yhteiskunnallisen luottamuksen heikkenemisellä tulee olemaan muilla yhteiskunnan osa-alueilla. On kuitenkin huomattava, että mikäli nämä osa-alueet otettaisiin mukaan, sen seuraukset tulisivat olemaan sitä vakavammat.

3.4. Johtopäätökset

Tämä luku on pyrkinyt tarkastelemaan disinformaatiota levittävien toimijoiden toimintaa kahdessa tapauksessa tapaustarkastelun kautta. Pääpaino on ollut erityisesti näiden toimijoiden käyttämillä keinoilla: Miten ne saavuttavat tavoitteensa, millaisia toimia niiden operaatioihin kuuluu ja miten ne käyttävät laskennallista propagandaa osana operaatioitaan. Yhdysvaltain senaatin tutkinta ja sitä tukevat tutkimukset tarjoavat kattavan kuvan siitä, miten Venäjä käytti laskennallista propagandaa vaikuttaakseen Yhdysvaltain 2016 presidentinvaaleihin, mutta myös laajemmin koko yhdysvaltalaiseen yhteiskuntaan. Sen toiminnan ytimessä olivat lukuisat valetilit ja sivustot, joiden kautta

[167] Ibid.
[168] WEF. 2020. *Fighting COVID-19 Could Cost 500 Times as Much as Pandemic Prevention Measures*. https://www.weforum.org/agenda/2020/08/pandemic-fight-costs-500x-more-than-preventing-one-futurity/., https://scitechdaily.com/economic-pain-covid-19-pandemic-will-cost-global-economy-21-trillion/., https://www.bbc.com/news/business-52671992

se pyrki luomaan lukuisia astroturffaus-kampanjoita. (Katso luku 4.6 astroturffaus-kampanjoista.) Valitettavasti tutkimuksen rajoitukset johtuen rajoitteista erityisesti Facebookin ja Googlen jakamassa datassa estävät jossain määrin tarkempaa analyysiä esimerkiksi sen kautta, käyttikö Venäjä amplifikaatioverkostoja näiden sivujen kasvattamiseen tai pyrkikö se hiljentämään kriittisten toimijoiden ääntä esimerkiksi suppression kautta? (Katso amplifikaatiosta ja suppressiosta lisää luvuista 4.2 ja 4.3.) Lisäksi ne eivät paljasta tarkasti automaation tasoa tai esimerkiksi bottitilien roolia Venäjän operaatiossa. Nojautuen kuitenkin aiempaan todistusaineistoon Venäjän vaikutus- ja disinformaatio-operaatioista muissa maissa, on hyvin todennäköistä, että myös nämä näyttelivät merkittävää roolia osana Venäjän operaatiota. Venäjä käytti kohdennettuja mainoksia sivustojen kasvattamiseen, mutta näiden mainosten rooli, ainakin jaetun datan pohjalta, oli kohtalaisen pieni kokonaisoperaatiolle.

Koronaviruspandemiaan liittyvä disinformaatio on laajalle levinnyttä ja tehokasta. Monet toimijat, näistä kenties merkittävimpinä Kiina ja Venäjä, levittävät disinformaatiota ja samalla pahentavat pandemiaa. Disinformaatiolla on yhteiskunnille ja sen kansalaisille todellinen hinta. Se heikentää institutionaalista luottamusta ja johtaa tilanteisiin, joissa yksilöt todennäköisemmin ohittavat viranomaisten antamien ohjeiden seuraamisen. Tämä osaltaan pahentaa pandemiaa ja sen seurauksena aiheuttaa merkittäviä kustannuksia yhteiskunnille mutta myös globaalille maailmantaloudelle. Nämä kustannukset mitataan ihmiselämässä kaksinkertaisesti, sekä viruksesta suoraan kuolleiden uhrien kautta että myös taloushaasteiden seurauksena ennenaikaisesti kuolleiden kautta. Disinformaation roolin kokoa osana ilmiötä on vaikea arvioida, mutta disinformaatio itsessään on laajalle levinnyttä, tehokasta ja hyvin yleistä. Myös kaksinaisseuraukset kuten heikentynyt luottamus instituutioihin ja viranomaisiin tulevat aiheuttamaan monenlaisia haasteita ja ongelmia, eivät vain pandemian yhteydessä vaan myös tulevaisuudessa.

Tässä yhteydessä on hyvä palata kysymykseen vastuusta. Ilman sosiaalista mediaa disinformaatio ei voisi levitä yhtä tehokkaasti, kattavasti tai laajalle eikä se välttämättä olisi yhtä uskottavaa.[169] Vaikka alustat itse eivät levitä disinformaatiota, ne ovat väline, jonka kautta se leviää. Samalla ilman niitä disinformaatio ei voisi levitä samalla tavalla. Tässä suhteessa disinformaatiota levittävät pahantahtoiset toimijat hyödyntävät alustojen

[169] Walsh, B. 2020. *Fighting the Coronavirus Infodemic*. Axios. https://www.axios.com/coronavirus-misinformation-conspiracy-theories-ad2785eb-b5a2-4ea5-8158-729cb8879130.html

laiskuutta ilmiötä vastaan taistelemisessa. Vaikka ne ovat ottaneet joitain askelia misinformaation tunnistamiseksi,[170] mis- ja disinformaation leviäminen itse kertoo, että toimet ovat olleet joko riittämättömiä tai epäonnistuneita ilmiön hallitsemiseksi. Toistaiseksi laskennallisen propagandan keinot ovat mahdollistaneet pahantahtoisille toimijoille keinot manipuloida alustoja, eivätkä alustat itse ole tehneet fundamentaalisia muutoksia tai ottaneet askeleita näiden laajamittaiseksi torjumiseksi.

Kenties realistisin vaihtoehto ilmiön hallitsemiseksi voisikin olla säädellä itse alustoja. Siinä missä pahantahtoisten toimijoiden katoaminen vaatisi todennäköisesti vähintäänkin maailmanrauhan ja todennäköisemmin laajamittaisen utopian sekä yhteiskunta- ja talousjärjestelmiemme täydellisen uudistamisen, alustojen säätely itsessään ei ole mahdotonta tai ennenkuulumatonta. EU:n 2018 voimaan saattama GDPR asetti merkittäviä uusia vaatimuksia alustoille esimerkiksi yksityisyyden suojelun suhteen. Samalla se näytti, että teknologiayritysten ja datan säätely on mahdollista. Kysymykseen vastuusta ja mahdollisista toimista alustojen suhteen palataan luvussa 5.

Seuraava luku, luku 4, menee syvemmälle laskennalliseen propagandaan erilaisten keinojen tarkastelun kautta eritellen erilaisia tunnistettuja laskennallisen propagandan keinoja ja menetelmiä sekä tarjoten todellisen maailman esimerkkejä näiden käytöstä. Tässä suhteessa se myös syventää kappaleen 3 tapauskuvausta erityisesti teknisestä näkökulmasta ja selittää paremmin erilaisten termien ja toimintatapojen mekanismeja ja tavoitteita. Luku 4 on myös työn teknisin luku, keskittyen erityisesti laskennallisen propagandan keinojen tuomiin mahdollisuuksiin todellisen maailman esimerkkien kautta.

4. Laskennallinen propaganda

Tähän mennessä työ on tutustunut yleisellä tasolla sekä eri toimijoihin että alustoihin. Tapauskuvauksen kautta se on luonut syvemmän katsauksen kahteen viimeisen vuosikymmenen merkittävimpään disinformaatiokriisiin. Luku 3 nosti esille tunnistettuja disinformaatiotoimijoita, kuten Kiinan ja Venäjän, joilla on ollut hyvin merkittävä rooli osana ilmiötä viimeisten vuosien aikana.

[170] https://www.nbcnews.com/tech/tech-news/facebook-says-it-labeled-50-millions-pieces-coronavirus-misinformation-april-n1205316

Luku neljä palaa kampanjoista laskennallisen propagandan keinoihin. Luku esittelee 10 laskennallisen propagandan keinoa ja ilmiötä sekä näiden keinojen ja ilmiöiden variaatioita tai alailmiöitä. Katsaus on teknisempi ja yksityiskohtaisempi kuin luvussa 3, mutta pyrkii myös sitomaan ilmiöt ja keinot konkretiaan lyhyiden esimerkkien kautta. Ilmiö ja keinokuvauksen rooli on myös siitä keskeinen, että laajamittaisia kuvauksia erilaisista keinoista teknisten ja konkreettisten esimerkkien kanssa on olemassa melko vähän. Useimmat työt kuvaavat ilmiötä tapaustutkimusten kautta, mutta keskittyvät hyvin harvoin kartoittamaan erilaisia tunnettuja keinoja tai kokoamaan näitä yhteen.

Luku aloittaa kuvauksen esittelemällä peruskäsitteitä erilaisista boteista ja algoritmien manipulointikeinoihin ja siirtyen käsittelemään ilmiöitä tuoreempien esimerkkien kuten potemkin-uutissivustoisojen kautta. Luvun viimeinen osio käsittelee sosiaalisen median mainontaa nostaen esille joitakin ilmiön ongelmia ja keskeisimpiä kehityssuuntia.

Luvun tarkoitus on auttaa lukijaa ymmärtämään ilmiön eri puolia erilaisten keinojen ja niiden luomien mahdollisuuksien näkökulmasta. Samalla se pyrkii selittämään, miten erilaiset keinot itseasiassa toimivat tai miten niitä käytetään. Tämän on tarkoitus tehdä työstä lähestyttävämmäksi kaikenlaisille lukijoille, aiemmasta taustasta riippumatta.

On myös tärkeää painottaa että luku ei sisällä täyttä listaa laskennallisen propagandan keinoista, eikä käsittele ilmiöitä kuten hashtagien myrkytys, A/B testaus tai psykometriikka. Laskennallisen propagandan ollessa hyvin laaja ja jatkuvasti kehittyvä ilmiö, täydellisen listan luominen ei tämän työn puitteissa ole mahdollista.

Luvun ensimmäinen osio, botit, käsittelee kenties laskennallisen propagandan ydinkäsitettä. Bottien rooli osana sekä sosiaalista mediaa että verkkoinfrastruktuuria on kasvanut merkittävästi viimeisinä vuosina. Vaikka kaikkia botteja ei käytetä negatiivisiin toimitarkoituksiin, ovat valitettavan monet toimijat valjastaneet botit palvelemaan synkempiä käyttötarkoituksia.

4.1. Botit

Botin määritelmä voi vaihdella merkittävästi eri tutkimusjulkaisujen, uutisartikkeleiden ja muiden raporttien välillä. Tällä hetkellä selkeää ja hyväksyttyä standardia bottien määrittelylle ja kategorisoinnille ei ole olemassa.

Botti on yksinkertaisimmillaan algoritmi, joka kykenee suorittamaan automatisoidusti tiettyä tehtävää. Ensimmäiset “web-botit”, niin sanotut ryömijät,[171] (crawler) kehitettiin, kun tietyllä sivustolla olevan informaation määrä alkoi ylittää yksittäisen käyttäjän resurssit kategorisoida ja organisoida manuaalisesti. Ryömijä oli web-botti, joka vieraili nettisivuston jokaisella sivulla ja linkillä sekä kategorisoi ja merkitsi näiden väliset yhteydet ja linkit toisille sivustoille. Nykyään termiä botti käytetään viittaamaan kaikenlaisiin automatisoituihin algoritmeihin, jotka suorittavat erilaisia tehtäviä. Botti on siis algoritmi, pätkä koodia, joka on ohjelmoitu automaattisesti suorittamaan tiettyä tehtävää.

Tyypillisiä käyttötarkoituksia botille nykyään ovat esimerkiksi uusien verkkosivujen kategorisointi (ryömijät, esimerkiksi hakusivustot kuten Google käyttävät näitä), uutisten seuranta ja levitys (uutisorganisaatiot soveltavat botteja käynnissä olevien tai juuri tapahtuvien uutisten seurantaan sekä uutistensa levitykseen) ja julkisesti saatavilla olevan tiedon luominen ja täydennys (Wikipedian kaltaiset sivut nojaavat merkittävissä määrin botteihin).[172]

Botteja käytetään merkittävissä määrin myös erilaisissa sosiaalisissa tehtävissä ja viime aikoina yhä useammat toimijat ovat alkaneet automatisoida asiakaspalveluaan soveltamalla botteja, jotka ohjaavat verkkoasiakkaita ja vastaavat yksinkertaisiin kysymyksiin.

Operoimalla useita botteja samanaikaisesti luodaan verkosto, johon viitataan tyypillisesti termillä bottiverkosto (botnet tai bot-networks). Bottiverkkoja voidaan käyttää moniin tarkoituksiin. Joissakin tapauksissa ne voivat esimerkiksi muodostua viruksen saaneista tietokoneista, jossa virus antaa yhden käyttäjän hallita näitä koneita ja joko generoida spammiä tai suorittaa DDoS-hyökkäyksiä (Luku 3.8 keskustelee DDoS-hyökkäyksistä). Toisaalta bottiverkostot voivat myös edistää poliittisia tavoitteita tai toimia yhdessä Twitterissä ja muilla sosiaalisen median alustoilla sisällön manipuloimiseksi tai muiden tavoitteiden saavuttamiseksi. Käytännössä bottiverkosto kuitenkin mahdollistaa usean

[171] Oma käännös. Alkuperäinen termi Crawler
[172] Howard, P., Woolley, S. & Calo, R. 2020. Algorithms, Bots, and Political Communication in the US 2016 Election: The Challenge of Automated Political Communication for Election Law and Administration. *Journal of Information Technology & Politics*. Vol 15. No 2.

botin ohjauksen samanaikaisesti, jolloin yksittäisen käyttäjän on mahdollista ohjata satoja, tuhansia tai kymmeniätuhansia botteja keskitetysti ja samanaikaisesti.

4.1.1. Botit sosiaalisessa mediassa

Sosiaalisessa mediassa bottien tarkoitus on yleensä esittää oikeaa käyttäjää. Toisin sanoen kyseessä on automatisoitu sosiaalisen median käyttäjä, joka on varustettu sisällön tuottamiseen sopivalla algoritmilla. Tämä käyttäjä kommentoi ja reagoi sisältöihin, jakaa sisältöä tai uutisia, lähettää yksityisviestejä, voi perustaa erilaisia ryhmiä ja kerätä seuraajia sekä kannatusta. Bottien tyypilliset toimintatarkoitukset sosiaalisessa mediassa vaihtelevatkin paljon ja laajasti, mutta voivat olla esimerkiksi tietyn sisällön näkyviin nostamista sen jakamalla ja siihen reagoimalla, propagandan jakamista julkaisemalla sitä itse ja jakamalla sitä seuraajilleen, uutistarinoiden levittämistä, keskusteluun vaikuttamista kommentoimalla tai reagoimalla, tai häiritsemällä sitä muilla keinoilla, sisältöjen massa-ilmiantamista, yksityisviestien lähettämistä toisille käyttäjille, käyttäjien seuraajamäärien ja näkyvyyden kasvattamista ja monia muita asioita.

Bottien profiilit voivat olla hyvin yksinkertaisia, vailla profiilikuvaa. Ne voivat antaa käyttäjänimekseen nimiä, joita tavallinen käyttäjä harvoin valitsisi, kuten sarjoja aakkosia ja numeroita ilman mitään merkitystä (esimerkiksi käyttäjänimi ‘374h8fjh6jk9’) ja esittää toiminnassaan selkeitä kaavamaisuuksia, jotka tekevät niistä helppoja tunnistaa botteja luokitteleville algoritmeille (lähettäen toistuvasti hyvin mekaanisia viestejä, toimien jatkuvasti vuorokausirytmistä riippumatta, lähettäen viestit toistuvasti samoihin aikoihin tai näyttäen muita hyvin selkeitä kaavoja käytöksessään, kuten suorittaen vain yhtä toimintatarkoitusta, esimerkiksi tiettyjen käyttäjien sisällön jakamista, tai vain lähettäen yksityisviestejä ja kommentointia, tai pelkästään julkaisten sisältöä, mutta ei koskaan reagoiden muuhun sisältöön.)

Toisaalta laadukkaat ja hyvin naamioidut botit voivat olla merkittävästi monimutkaisempia ja vaikeampia tunnistaa. Poliittiset toimijat ja kyberjoukot käyttävät jatkuvasti hienostuneempia ja kehittyneempiä botteja, jotka tekevät niiden luokittelusta vaikeaa. Ne seuraavat vuorokausirytmiä, välttävät selkeitä kaavamaisuuksia, omaavat aidontuntuiset ja monipuoliset profiilit sekä osallistuvat lukuisiin eri toimintamuotoihin, sen sijaan että ne osallistuisivat vain yhteen hyvin spesifiin toimintaan.

4.1.2. Hybridibotit, yksinkertaiset botit ja bottiverkot

Bottien tunnistaminen sosiaalisessa mediassa on tyypillisesti ollut merkittävä ongelma. Tunnistusmetodien kehittyessä myös botit kehittyvät hienostuneemmiksi, vaikeammiksi tunnistaa ja monipuolisemmiksi. Tosin tutkijoilla ei ole yhteisesti hyväksyttyä standardia bottien luokitteluun, esimerkiksi bottien ja ei-bottien välillä voidaan tehdä jonkin verran erottelua käyttämällä tyypillisesti automaation määrään sekä botin julkaiseman sisällön luomismetodia. Erottelu on tarpeellista tehdä esimerkiksi ihmiskäyttäjien, hybridibottien, yksinkertaisten bottien, hybridibotti-verkostojen ja yksinkertaisten bottien verkostojen välille.

Tyypillinen ihmiskäyttäjä ilmentää hyvin matalan järjestäytymistason eikä tyypillisesti ilmennä automaatiota osana toimiaan.

Yksinkertainen botti on täysin automatisoitu sekä toiminnassaan että siinä, miten se tuottaa sisältöä. Sen tuottama sisältö on helposti tunnistettavissa eikä ole laadullisesti kovin tehokasta ihmiskäyttäjien pettämisessä (tarkoittaa sitä, että käyttäjän on helppo nähdä sisällön olevan botin kirjoittamaa eikä orgaanista.) Se pystyy kuitenkin joihinkin automatisoituihin toimiin tehokkaasti.

Hybridibotti on välimuoto, joka yhdistää botin automaatiota ihmiskäyttäjään. Sen toiminta on automatisoitua, mutta se pyrkii tyypillisesti imitoimaan ihmiskäyttäjää omaten vuorokausirytmin, aktiivisuusajat sekä seurantakäytöksen. Sen sisältö on kuitenkin ihmisten tuottamaa ja näin sekä laadukkaampaa että uskottavampaa.

Yksinkertainen bottiverkosto on keskitetyltä serveriltä ohjattu verkko botteja, jotka käyttäytyvät hyvin samankaltaisesti omaten hyvin pienen määrän autonomiaa toimissaan.

Hybridibottiverkosto on yhtä lailla keskitetyltä serveriltä ohjattu verkosto. Erona kuitenkin on, että hybridibotit omaavat käytöksellisen autonomian, jonka avulla ne pyrkivät imitoimaan ihmiskäytöstä.

[173]

Bottien toiminta- ja käyttöstrategioista keskustellaan enemmän tämän työn myöhemmissä luvuissa, esimerkiksi luvussa 3.2, 3.3 ja 3.5 ja 3.6.

[173] Grimme, C., Preuss, M., Adam, L. & Trautmann, Heike. 2017. *Social Bots: Human-Like by Means of Human Control?* https://arxiv.org/pdf/1706.07624.pdf

4.2. Amplifikaatio

Amplifikaatio, voimistaminen, tarkoittaa signaalien vahvistamista. Tämä on yksi yleisimmistä ja eniten käytetyistä sisällön manipulaation muodoista. Amplifikaatio nojaa sosiaalisen median palvelujen sisältöalgoritmien manipulointiin ja hyödyntää valekäyttäjien kautta toimivia botteja työkaluina mahdollistamassa toimintaa. Tavallisia amplifikaation kohteita ovat käyttäjien julkaisut, uutiset, videot tai itse käyttäjät.

Amplifikaatio voi ottaa toimintastrategiana useita muotoja. Käytetty toimintastrategia riippuu tyypillisesti toimijan tavoitteista sekä teknisistä että taloudellisista resursseista, ja myös toimialustasta ja olosuhteista. Tässä luvussa käsitellään kahta amplifikaation muotoa, joista toinen tähtää nostamaan yksittäistä toimijaa ja toinen keskittyy laajemmin tietyn agendan ajamiseen. On myös huomattava, että vaikka tässä luvussa nämä muodot käsitellään erillisinä osioina, niitä voidaan hyvin käyttää sekaisin toistensa kanssa tai yhdessä eikä rajanveto sosiaalisessa mediassa tyypillisesti ole näinkään selkeää edes tarkoitusperien tai toimintastrategioiden suhteen.

Ensimmäinen käytetty amplifikaation muoto on amplifioida yksittäisiä henkilöitä ja heidän julkaisujaan. Julkaisujen näkyvyyttä voidaan parantaa ohjaamalla botteja reagoimaan ja jakamaan julkaisua heti sen ilmestymisen jälkeen. Tämä toimii kahdella tasolla: Riippuen bottien omista verkostoista, julkaisu nousee näkyväksi ja se jaetaan näissä verkostoissa niiden seuraajille ohjaten enemmän ihmisiä näkemään alkuperäisen julkaisun, riippuen toki bottien omista verkoista. Toisaalta valekäyttäjien eli bottien reaktiot myös nostavat julkaisun ”trendingiä”. Johtuen siitä miten sosiaalisen median sisältöalgoritmit toimivat, [174] julkaisujen näkyvyyteen vaikuttaa merkittävästi se, kuinka monia reaktioita se pystyy saamaan tietyssä ajassa. Bottien tarkoitus on siis ohjata omat reaktionsa voimistamaan julkaisun näkyvyyttä, mutta myös jakaa jo amplifioitua julkaisua omien verkostojensa kautta. Mitä laajempia bottien omat verkostot ovat (mitä enemmän aitoja, muista käyttäjistä muodostuvia seuraajia niillä on) sitä tehokkaampaa tämä toiminta on.

[174] (se, kuinka monille ihmisille sivusto näyttää julkaisun ja kuinka korkealle julkaisu sijoittuu heidän “feedissään”, tai syötteessään, on itseasiassa hyvin monimutkainen kysymys, johon ei ole täysin selkeää vastausta, sillä alustat suojelevat sisältöalgoritmiensa yksityiskohtia äärimmäisen tarkasti. Tiedetään kuitenkin yleisellä tasolla että paljon reaktioita lyhyeen aikaan vetävä julkaisu nousee trendingissä. Twitterissä riittävän vahvasti trendaavan julkaisun #hashtag voi jopa nousta maan top 100 trending hashtags listalle, jolloin se saa näkyvyyttä myös riippumatta käyttäjän omista seuraajista tai seurannasta.)

Tämänkaltaisen toimintastrategian käyttö on tunnistettu esimerkiksi Venezuelassa, missä tutkijat ovat havainneet, että jopa 10 prosenttia useiden poliitikkojen julkaisujen jaoista tulee boteilta.[175] Vaikka tutkijat ovat kuvanneet ilmiötä vaikeasti havaittavaksi, on todennäköistä, että sillä on merkittävä, jos tosin huomaamaton vaikutus Venezuelan Twitterissä käytävään poliittiseen dialogiin.

Toinen amplifikaation muoto on tietynkaltaisen sisällön nostaminen riippumatta niinkään sen lähteestä. Tällöin tarkoituksena ei ole nostaa yksittäisen toimijan vaan tietyn asiakysymyksen tai laajemman agendan näkyvyyttä ja saada sille kannatusta. Jotkin tässä osiossa käsitellyt teemat nousevat esille myös luvussa 3.6, astroturffaus. Siinä missä yksittäisen henkilön amplifioiminen nojaa yleensä tämän henkilön omien julkaisujen jakamiseen ja näihin reagoimiseen (toki sen ei tarvitse rajoittua tähän toimintaan), tietyn agendan tai asiakysymyksen nostamista voidaan toteuttaa vähemmän keskitetysti niin, ettei sen tarvitse nousta tietystä lähteestä. Tässä erityisen hyödylliseksi tulevat kehitetyt, laajan seuraajakunnan omaavat hybridibotti-verkostot, jotka voivat jakaa informaatiota itsenäisesti nojaamatta jo valmiiksi olemassa olevaan käyttäjään tai auktoriteettiin. Botti- tai hybridibotti-verkosto, jolla on laaja seuraajakunta,[176] voi yksin levittää viestejä tehokkaasti Twitterin tai Facebookin kaltaisissa toimintaympäristöissä tarvitsematta ulkoista voimistajaa tai jo valmiiksi näkyvää ja laajan seuraajakunnan omaavaa henkilöä, jonka viestejä se voi jakaa. Itseasiassa bottiverkostot ovat hyvin tehokkaita valeuutisten, disinformaation ja poliittisten näkemysten jakajia.

Keskeinen haaste amplifikaation näkökulmasta on bottiverkostoon kuuluvien bottien laatu sekä niiden profiilien että seurantamäärien suhteen. On tyypillisesti helpompaa ja vähemmän resursseja kuluttavaa rakentaa laaja bottiverkosto, joka pystyy amplifioimaan viestejä tarjoamalla reaktioita ja uudelleenjakoja. Ongelmana kuitenkin on, että tällaisen

[175] Forelle, M., Howard, P., Monroy-Hernández A. & Savage, S. 2020. *Political Bots and the Manipulation of Public Opinionin Venezuela*.

[176] (yksittäisellä tai yksittäisilä boteilla voi olla tuhansien, kymmenien tuhansien tai jopa satojen tuhansien käyttäjien seuraajakunta Twitterissä. Tosin hyvin laajojen, yli kymmeniin tuhansiin yltävien seuraajakuntien kasvattaminen on haastavampaa ja vaatii merkittävämpää teknistä ja sisällöllistä osaamista bottien operoijilta. Bottiverkostojen koot myös tyypillisesti pienenevät bottien omien seuraajakuntien kasvaessa tai ne voivat toimia tehokkaasti ja saavuttaa kokonaisen bottiverkoston tehtävän yksin.)

verkoston bottien uudelleenjaot eivät ole yhtä arvokkaita, mikäli ne eivät omaa itse merkittäviä seuraajamääriä.

Vuoden 2017 tutkimuksessaan Grimme ym. testasivat, miten helppoa olisi rakentaa 30 botille seuraajaverkko Twitterissä. Noin kahdeksan päivän aikana tutkijat onnistuivat rakentamaan 1350 seuraajan verkoston, mikä osoitti tasaista kasvua koko tutkimusjakson ajan. Käyttämällä verkostoa tutkijat onnistuivat myös saamaan yhden bottien kautta jakamistaan hashtageista ilmenemään Saksan top 100 ”trendaavan” hashtagin listalla. Osana kokeen loppuvaihetta tutkijat paljastivat bottien seuraajille niiden henkilöllisyyden. Tästä tutkijat pystyivät selvittämään, että merkittävä osuus niiden seuraajista ei ollut pystynyt havaitsemaan käyttäjiä boteiksi. Tutkijat itse arvioivat bottiverkoston luomiseen ja kasvattamiseen liittyvän työmäärän ja teknisen osaamisvaatimuksen “merkityksettömän pieneksi” (“Negligible”). [177] Samalla tutkimus myös osoittaa realistiseksi laajempien, kauemmin kehitettyjen ja kasvatettujen seuraajaverkostojen luomisen Twitterissä bottiverkostoille. Näin se osoittaa, että tällaisten verkostojen on mahdollista levittää sisältöä tehokkaasti ja vaikuttaa ”trendaaviin” #hashtageihin ja hämätä oikeita käyttäjiä.

Näiden tutkimusten lisäksi amplifikaatiosta löytyy lukuisia todellisen maailman esimerkkejä. Useat firmat, mukaan lukien jotkin poliittiset konsultointi- ja viestintäyritykset, tarjoavat nykyään asiakkailleen palveluita, joiden tarkoituksena on nostaa julkaisujen näkyvyyttä ja kasvattaa seuraajamääriä sekä Twitterissä että Facebookissa.[178]

4.3. Suppressio

Suppressio, sisällön tai käyttäjän johdonmukainen vaimentaminen, hautaaminen tai hiljentäminen, viittaa toimintaan, jonka tarkoituksena on häiritä keskustelua, peittää tietynlaista sisältöä tai hiljentää joku keskustelija.

[177] Grimme, C., Preuss, M., Adam, L. & Trautmann, Heike. 2017. *Social Bots: Human-Like by Means of Human Control?* https://arxiv.org/pdf/1706.07624.pdf

[178] Bay, S.& Fredheim, R. 2019. *Falling Behind: How Social Media Companies Are Failing to Combat Inauthentic Behaviour Online.* NATO STRATCOM COE.

Tietynlaisen sisällön suppressointiin voi olla monia keinoja. Ne riippuvat alustasta, sisällön levinneisyyden laajuudesta tai siitä, millaisessa kontekstissa ja millä skaalalla toimitaan. Suppressiosta voidaan puhua laskennallisen propagandan kontekstissa sekä keinona että strategiana, jolloin sen menetelmät vaihtelevat hiukan.

Suppressio keinona viittaa enemmänkin äänten ja näkyvyyden manipulointiin, jolloin esimerkiksi erilaisilla foorumityyppisillä alustoilla se voidaan saavuttaa yksinkertaisella äänimanipulaatiolla. Useimmat sosiaalisen median alustat eivät anna käyttäjien esittää algoritmin näkökulmasta suoranaisen negatiivisia reaktioita (tarkoittaen tykkäykselle suoraan vastakkaista reaktiota, joka laskisi julkaisun näkyvyyttä sen nostamisen sijaan). Toisaalta alustat kuten Reddit, jotka mahdollistavat suoraan vastakkaiset ”ylös”- ja ”alas”-äänet, tekevät sisällön systemaattisesta suppressiosta ja manipulaatiosta helppoa juuri äänimanipulaation kautta. Yksittäisen tai useampien julkaisujen näkyvyyden manipulointiin riittää tarpeeksi suuri määrä valekäyttäjiä, jotka kohdistavat strategisia ”alas”-ääniä sisällölle, joka halutaan saada pois näkyvistä. Tätä voidaan täydentää strategisesti nostamalla näkyvyyttä sellaisessa sisällössä, jonka halutaan tai harhauttavan toisesta sisällöstä. Tarpeen vaatiessa voidaan myös soveltaa botteja, jotka vahtivat tiettyjä avainsanoja ja aihealueita ja automatisoivat prosessin tai vain mahdollistavat suuremmat määrät ”alas”-ääniä.

Toisilla alustoilla sisältöä on mahdollista pyrkiä vaimentamaan esimerkiksi astroturffauksen tai DDoS-hyökkäysten kautta. Astroturffaus voisi pyrkiä hyvin vihamielisiin ja negatiivisiin reaktioihin, joiden tarkoituksena olisi vaikuttaa mielikuvaan tai näkyvyyteen aiheesta tai kilpailevien julkaisujen luomiseen, joiden tarkoituksena olisi vaikuttaa lukijan kuvaan aiheesta. DDoS-hyökkäys pienempään verkkosivustoon voisi pyrkiä tiedonsaannin katkaisuun strategisella hetkellä, leviämisen estämiseen tai vain toiminnan yleiseen häiritsemiseen ja vaikeuttamiseen. (Katso aiheista lisää luvuista 4.3, 4.5)

Eräs tyypillisesti käytetty suppression keino on tehdä ilmiantoja julkaisusta. Alustat kuten Facebook ja Twitter, joissa jokainen julkaisun tuottama reaktio nostaa sen asemaa niiden käyttämässä sisältöalgoritmissa, tyypillinen toimintatapa voi olla julkaisun massailmiantaminen alustalle. Tämä toimintatapa on tehokas johtuen Facebookin ja Twitterin käyttämästä automatisoidusta sisällönvalvonnasta. Esimerkiksi Facebook

soveltaa niin kutsuttua reaktiivista sisällönvalvontaa. Tämä tarkoittaa, että sen sijaan että se proaktiivisesti moderoisi alustallaan julkaistua sisältöä varmistaen sen olevan ehtojensa mukaista, se luottaa käyttäjiensä ilmoituksiin epäsopivasta tai ehtoja rikkovasta sisällöstä. Tällöin huomattava määrä ilmoituksia yksittäisestä julkaisusta (kymmeniä tai satoja lyhyen ajan sisällä) johtaa automaattisesti sen sisällön poistamiseen sekä mahdolliseen varoitukseen käyttäjälle riippumatta siitä, mikä itse julkaisun sisältö oli. Käyttäjän on mahdollista pyytää alustaa uudelleenarvioimaan tapausta, joka laukaisee arviointiprosessin, jossa alustan työntekijä uudelleenarvioi julkaisun sisällön sekä poistamisen kontekstin.

Mikäli havaitaan, että ilmoituksen olivat perusteettomia, sisältö voidaan palauttaa sivustolle. Tämä kuitenkin vaatii käyttäjää itse proaktiivisesti ottamaan yhteyttä sivuston käyttäjäpalveluun, minkä lisäksi prosessi voi kestää joitakin päiviä. Se antaa myös tällaisille hyökkäyksille merkittävän määrän valtaa, sillä ne voivat, ainakin hetkellisesti, sensuroida toisten käyttäjien julkaisuja ja puhetta verkossa. Tällaisen hyökkäyksen kohteeksi joutuminen voi myös käyttäjälle olla pelottavaa, harmittavaa tai turhauttavaa ja vaikuttaa hänen verkkokäyttäytymiseensä jatkossa. Menetelmä tunnetaan myös nimellä DDoS 2.0. (DDoS-hyökkäyksiä kuvataan tarkemmin luvussa 4.8.)

Tyypillisesti käyttäjään kohdistuvat suppressio-hyökkäykset ovat hyvin vihamielisiä. Pyrkimyksenä on usein kohdistaa hyökkäys suoraan henkilön persoonaan. Tyypillisesti tällöin tarkoitetaan tilannetta, jossa joko yksittäinen käyttäjä (mikäli suppressio tai hyökkäys kohdistuu ensisijaisesti virtuaaliseen persoonaan) tai yksityinen henkilö (jos hyökkäys kohdistuu ensisijaisesti henkilön todelliseen persoonaan) pyritään hiljentämään häirinnän, pelottelun, uhkailun tai vaimennuksen kautta. Tällöin on tyypillistä soveltaa laajasti laskennallisen propagandan keinoja, riippuen kohteesta. Doksaus, trollaus tai muu häirintä kuten vihapuhe, henkilön tai hänen perheenjäseniinsä kohdistuvat uhkaukset sekä toistuvat ja häiritsevät yhteydenotot ja yksityisviestit. Joskus myös henkilön menneisyydestä löytyvien yksityiskohtien julkaiseminen ja levittäminen tiettyjen ryhmien keskuuteen voi olla toimiva keino.

Kuvauksia systemaattisen häirinnän kohteeksi joutuneiden henkilöiden kokemuksista on lukuisia. Tyypillisiä uhreja ovat aktivistit, journalistit tai muut kansalaisyhteiskunnan edustajat, sekä poliitikot ja viranomaiset. Toimijat voivat olla joko poliittisia kampanjoita

(tällöin tyypillisesti pyritään toimimaan lain rajoitteiden sisällä) tai valtiollisia tai valtioiden tukemia kyberjoukkoja, yrityksiä tai muita toimijoita. Esimerkiksi Trumpin kampanjan kerrotaan käyttävän näitä menetelmiä aktiivisesti.

Donald Trumpin kampanjan kerrotaan vuosien aikana keränneen merkittävän määrän tietoa politiikan toimittajista, näkyvistä akateemikoista, poliitikoista, julkisuuden henkilöistä sekä muista potentiaalisista henkilöistä. Heidän sosiaalisen median käyttäjiään, uutisjulkaisujaan ja muita virtuaalisia jalanjälkiä on käyty läpi useiden vuosien aikajaksolla. Epämiellyttävän uutistarinan noustessa kampanjan lähellä toimivat henkilöt käyvät läpi tietokannan tarinan kirjoittaneesta henkilöstä. Mikäli tietokanta sisältää jotain hyödyllistä kuten esimerkiksi ongelmallisen vanhan vitsin tai todisteen epäsopivista poliittista näkemyksistä, kampanja ohjeistaa tuttua uutissivustoa kirjoittamaan tästä uutisen, jonka kampanjan jäsenet voivat jakaa sosiaalisen median tileillään. Eräs uutisoiduista uhreista oli John Haltwingerin, *Business Insider*-lehdessä työskentelevä toimittaja. Kyseinen toimittaja oli julkaissut twiitin, joka veti Trumpin kampanjan huomion puoleensa.[179]

Tämän seurauksena kampanja julkaisi tarinan *Breitbart Newsin*. Tarina oli sarja Instagram-julkaisuja, jotka kyseinen henkilö oli tehnyt ennen työllistymistään *Business Insiderilla*, joissa hän oli pilkannut Trumpia ja ilmaissut sympatisoivansa liberaalien protestoijien kanssa. Tarinan julkaisun jälkeen, Donald Trump Jr. jakoi tarinan noin 3 miljoonalle seuraajalleen. Tämä johti useisiin vihaisiin ja uhkaileviin viesteihin, sekä satoihin yhteydenottoihin, jotka vaativat hänen irtisanomistaan. *Business Insider* antoi Haltwingerin säilyttää työnsä, mutta julkaisi lausunnon, jossa se totesi, etteivät Haltwingerin Instagram julkaisut “olleet sopivia” (“Not appropriate”.) Arviot tietokannan koosta vaihtelevat. Konservatiivisimmat arviot sijoittavat sen muutamaan sataan henkilöön, kun taas toiset kertovat sen sisältävän tietoa yli 2000 henkilöstä.[180]

4.4. Valeuutiset ja vale-uutissivustot

Valeuutisia tarkastellaan erityisesti niiden välinearvon kautta menetelmänä tässä luvussa.

[179] https://www.nytimes.com/2019/08/25/us/politics/trump-allies-news-media.html., https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530/.
[180] Ibid.

Valeuutiset ovat olleet jo pitkään näkyvillä myös mediassa. Aihe on tyypillisesti paremmin tunnettu. Valeuutisilla ja laajemmin niitä levittävillä uutissivustoilla, on kuitenkin merkittävä rooli osana laskennallista propagandaa, joka on noussut esille viime aikoina erityisesti Yhdysvalloissa.

Valeuutiset laskennallisen propagandan keinona toimivat selkeästi roolissa, jossa niillä on merkittävää välinearvoa. Valeuutinen tässä kontekstissa on tyypillisesti kirjoitettu palvelemaan tiettyä tarkoitusta. Sen levittäminen ei välttämättä ole itsetarkoitus (tosin se voi olla), mutta tyypillisemmin se tarjoaa valheellisen tai väärennetyn dialogin tapahtumasta, jolla voidaan haastaa totuus. Tässä suhteessa valeuutiset voivat olla joko osittain tai kokonaan valheellisia keksien kokonaan uusia väitteitä, tapahtumia tai tosiseikkoja. Vaihtoehtoisesti ne voivat ottaa todellisen tapahtuman ja taivuttaa totuutta esimerkiksi kertoen selkeästi valheellisen tai harhaanjohtavan tarinan, mutta käyttäen faktoja sen tekemiseen. Valeuutiset saattavat siis olla nimenomaan tiettyyn tarkoitukseen kirjoitettuja, poliittista agendaa palvelevia julkaisuja. Tarkoituksena voi olla esimerkiksi tiettyyn uutiseen vastaaminen, kilpailevan tarinan luominen tietystä asiakysymyksestä tai tapahtumasta tai vain totuuden hämärtäminen.

Yhtenä esimerkkinä voidaan käyttää usein oikean siiven uutissivustojen tekemiä ja Trumpin kampanjan sosiaalisessa mediassa jakamia videoita 2019 virkarikostutkintaprosessin aikana. Kommunikoidessaan prosessista, kampanja käytti videoita, jotka oli editoitu tavalla, joka sai lopputuloksen ilmenemään hyvin erilaisella tavalla kuin alkuperäisen videon konteksti antaisi katsojan ymmärtää. Leikkaamalla suurimman osan videosta, hyvin langettava lausunto päivän tapahtumista voitiin saada näyttämään siltä, että Trumpin tuomitsemisen sijaan se julisti tämän syyttömyyttä.[181]

4.4.1. Potemkin-paikallissivustot (tai vale-uutissivustot)

Toinen, vähemmän tunnettu ja valeuutisiin liittyvä, erityisesti viimeisen kahden vuoden aikana Yhdysvaltojen politiikassa noussut ilmiö ovat paikalliset valeuutissivustot tai Potemkin-paikallisuutissivustot. Strategia nojaa siihen, että Yhdysvalloissa kansalaiset ovat perinteisesti luottaneet paikallisuutisiin enemmän kuin kansallisiin uutisiin.[182]

[181] https://www.theatlantic.com/magazine/archive/2020/03/the-2020-disinformation-war/605530/
[182] The John S. And James L. Knight Foundation. 2019. *State of Public Trust in Local News*.

Vuonna 2020 julkaistu Pew Research Centerin tutkimus kertoi, että noin 72 % aikuisista Yhdysvalloissa seuraa aktiivisesti paikallisen median uutisointia.[183]

Termillä Potemkin-paikallisuutissivustot tarkoitetaan uutissivustoja, jotka pyrkivät uutisoinniltaan ja ulkonäöltään sekä nimeltään muistuttamaan paikallisia uutissivustoja, mutta ovat todellisuudessa keskitetysti luotuja ja operoituja faux-uutissivustoja. Tähän mennessä Potemkin-paikallisuutissivustoja on Yhdysvalloissa tunnistettu noin 450 kappaletta. Näiden taustalla on tunnistettu viisi ne omistavaa mediayritystä. Suurimmat toimijat Yhdysvalloissa ovat Franklin Archer, Metric Media ja LocalLabs, jotka yhdessä operoivat vuoden 2019 lopussa noin 70 % valesivustoista.[184]

Sivustot julkaisevat pääasiassa automaattisesti tuotettua sisältöä, joka ei sisällä kirjoittajan nimeä tai muuta tunnistetietoa. Monet niistä tulevat automatisoiduilta palveluilta (kuten Metric Media News Service tai Local Labs News Service). Ne käyttävät lähteinään esimerkiksi erilaisten valtiollisten virastojen datajulkaisuja tai muiden paikallisten julkaisujen muokattuja uutisia sekä kansallisuutisten tiedoksiantoja. Sivustojen uutissisältö muodostuu siis hyvin suurelta osalta automaattisesti tuotetuista, alueellisista ja kansallisista uutisista, jotka voidaan tuottaa hyvin pienellä määrällä resursseja. Näin sivustojen ylläpito voidaan automatisoida lähes kokonaan. Tällä tavalla sivustoista saadaan uskottavan ja aidon näköisiä sekä tuntuisia paikallissivustoja muistuttavia uutislähteitä.[185]

Useat sivut ovat uutisoineet valheellisista paikallisuutissivustoista. Michigan Daily, The New York Times, The Guardian ja Lansing State Journal ovat tunnistaneet sivuja ja uutisoineet niiden olemassaolosta ja toiminnasta.[186] Sivustoja yhdistäviä tekijöitä ovat

---

[183] Miller, C., Purcell, K. & Rosenstiel. T. 2012. *72% of Americans Follow Local News Closely.* Pew Research Center.

[184] https://www.cjr.org/tow_center_reports/hundreds-of-pink-slime-local-news-outlets-are-distributing-algorithmic-stories-conservative-talking-points.php

[185] https://www.cjr.org/tow_center_reports/hundreds-of-pink-slime-local-news-outlets-are-distributing-algorithmic-stories-conservative-talking-points.php., https://www.michigandaily.com/section/community-affairs/pseudo-local-news-sites-michigan-reveal-nationally-expanding-network., https://www.nytimes.com/2019/10/31/upshot/fake-local-news.html.

[186] https://www.michigandaily.com/section/community-affairs/pseudo-local-news-sites-michigan-reveal-nationally-expanding-network., https://www.theguardian.com/us-news/2019/nov/19/locality-labs-fake-news-local-sites-newspapers., https://www.nytimes.com/2019/10/21/us/michigan-metric-media-news.html., https://www.lansingstatejournal.com/story/news/local/2019/10/21/lansing-sun-new-sites-michigan-local-news-outlets/3984689002/.

tyypillisesti oikealle nojaava, konservatiivinen agenda sekä joitakin yksittäisiin asiakysymyksiin puuttuvia huomioita. Columbia Journalism Reviewin julkaiseman tutkimuksen mukaan sivustot ottivat usein kantaa yksittäisiin asiakysymyksiin. Kannanotot olivat usein lainauksia puolueen näkyviltä hahmoilta kuten osavaltion senaattorilta tai kongressinedustajalta. Jotkin artikkelit yrittivät mustamaalata istuvaan presidenttiin kohdistuvaa virkarikostutkintaa kutsuen Trumpiin kohdistuvaa virkarikostutkintaa noitavainoksi tai demokraattien vallan väärinkäytöksi.[187]

Potemkin-sivustoista on tullut osa poliittisen propagandan levitystä. Ne yhdistävät korkean automatisaation, algoritmien käytön ja samalla toimivat puhetorvena niitä ohjaileville tahoille. Toisin kuin perinteinen uutissivusto, se ei tarvitse yhtä tai useampaa toimittajaa ja editoria työskentelemään sivun parissa. Yksi henkilö voi automatisoitujen sisällöntuottotyökalujen kautta todennäköisesti hallinnoida useampaa sivua samanaikaisesti. Sivustot naamioituvat paikallisiksi sanomalehdiksi ja pyrkivät hyödyntämään yhdysvaltalaisten tunnetusti korkeampaa luottamusta paikallisuutisiin ja -sanomalehtiin. Sivustojen luojat ovat tyypillisesti media-alan tai viestinnän konsultointiyrityksiä. Toistaiseksi ilmiö on liitetty vain republikaanisen puolueen agendaan ja poliitikkoihin.[188]

4.5. Astroturffaus

Astroturffaus, (tai vähemmän tunnetulta suomenkieliseltä nimeltään ruohomattoilu) tarkoittaa järjestettyä toimintaa, jonka tarkoitus on pyrkiä imitoimaan ruohonjuuritasolla tapahtuvan toiminnan tunnuspiirteitä yrittäen luoda vaikutelman spontaanista ja aidosta ilmaisusta. Astroturffauksesta alettiin puhua laajemmin tutkimuksen parissa 1990-luvulla tutkijoiden alkaessa tunnistaa lobbauksen parissa ilmenevää uutta vaikutusmuotoa, ruohomattolobbausta (astroturf-lobbying). Se muistutti ruohonjuuritason kansalaistoimintaa, mutta oli itseasiassa tuotettua ja valheellista.[189]

[187] https://www.cjr.org/tow_center_reports/hundreds-of-pink-slime-local-news-outlets-are-distributing-algorithmic-stories-conservative-talking-points.php
[188] Potemkin-uutissivustoja: https://hickorysun.com/, https://nemontananews.com/, https://lansingsun.com/, https://grandrapidsreporter.com/, https://annarbortimes.com/, https://greatlakeswire.com/
[189] Savage, A., 1995. Astroturf lobbying replaces grassroots organizing. *Business and Society Review*. p. 8-10

Vuosituhannen lopussa Yhdysvaltojen poliittisen lobbauksen alueella alettiin tutkimaan muita vaihtoehtoja ruohonjuuritason lobbaukselle. Vaikka toiminta oli tehokasta, se oli jossain määrin resurssi-intensiivistä ja haastavaa. Seuraava askel prosessissa oli luopua tavallisista kansalaisista osana prosessia. Sen sijaan että astroturf-lobbarit yrittäisivät manipuloida tavallisia kansalaisia kohdistaakseen heidän huomionsa asiakysymykseen ja voidakseen näin vaikuttaa poliittiseen prosessiin, toimijat tajusivat voivansa luopua vaikeasti hallittavasta ja organisoitavasta välikädestä tuottamalla sen itse.[190] Tämä tapahtui sponsoroimalla eturyhmäjärjestöjä tai perustamalla niitä itse, kirjoittamalla kuluttajien puolesta kirjeitä, joissa he ilmaisivat kannatuksensa asian puolesta tai sitä vastaan tai muuten luomalla kannanottoja esimerkiksi lehtimainosten, järjestettyjen protestien (joissa osanottajat on palkattu osallistumaan tapahtumaan) tai puhelinkampanjoiden kautta.[191]

Astroturffaus sosiaalisen median kontekstissa on perusidealtaan samanlaista mutta sovitettuna digitaaliseen toimintaympäristöön ja sen mahdollisuuksiin. Ilmiötä on vaikea määritellä kattavasti, mutta Kovic ym. tarjoama määritelmä “tuotettua, harhaanjohtavaa ja strategista, ylhäältä ohjattua toimintaa, jonka tarkoitus on imitoida autonomisten yksilöiden ruohonjuuritasolta nousevaa toimintaa" kuvaa sitä hyvin.[192] Keinona astroturffauksen tarkoitus on siis kaikissa muodoissaan imitoida autonomisten yksilöiden mielipiteistä nousevaa ilmaisua ja imitoida tällaisia heikkoja signaaleja, joihin ainakin yhdysvaltalaisessa kontekstissa erityisesti poliitikkojen tiedetään kiinnittävän huomiota.[193]

Sosiaalisessa mediassa astroturffaus ottaa tyypillisen keskitetysti ohjatun kampanjan muodon, jossa toimija pyrkii imitoimaan toista henkilöä, organisaatioita, ryhmää tai toimintaa. Käytännössä valekäyttäjät julkaisevat astroturffaus-kampanjan agendalle myönteistä sisältöä ja pyrkivät hallitsemaan keskustelua muun muassa yrittämällä

---

[190] Lyon, T. & Maxwell, J. 2002. *Astroturf Lobbying.*
[191] Deal, C. & Doroshow, J. 2003. Corporate Astroturf and Civil Justice. *Multinational Monitor; Washington*. Vol. 24, No. 3.
[192] Kovic, M., Rauchfleisch, A., Sele, M. & Caspar, C. 2018. Digital Astroturfing in politics: Definition, Typology, and Countermeasures. *Studies in Communication Sciences.* Vol 18. No.1
Oma käännös. Alkuperäinen versio: “We propose to call such fake online grassroots activity digital astroturfing, and we define it as a form of manufactured, deceptive and strategic top-down activity on the Internet initiated by political actors that mimics bottom-up activity by autonomous individuals”
[193] Lohmann, Suzanne. 1993. A Signaling Model of Informative and Manipulative Political Action. *American Political Science Review*, p. 87., Krishna, Vijay and John Morgan. 2001. A Theory of Expertise. *Quarterly Journal of Economics*, p. 116.

harhauttaa käyttäjiä negatiivisista näkökulmista, vetämällä huomiota jakolinjoja aiheuttaviin poliittisiin kysymyksiin tai hyökkäämällä vastustajia ja kriitikoita vastaan.[194] Tämä on myös Venäjän vaikutusoperaatioiden laajasti käyttämä manipulaatiomenetelmä, joka oli integraalinen erityisesti sen Yhdysvaltojen kampanjalle, joka nojasi lukuisiin valesivuihin sekä käyttäjiin. (Katso tarkemmin luvusta 3.1)

Kampanjat voivat soveltaa joko botteja, ihmiskäyttäjiä ja trollifarmeja tai hybridibotteja ja automaatioavusteisia kyborgikäyttäjiä (pitkälti sama asia kuin hybridibotti). Valinta riippuu pitkälti kampanjan tarpeista, resursseista sekä siitä, kuinka suurta määrää käyttäjiä tulee operoida yhtäaikaisesti ja kuinka suuri vaikutus halutaan saada aikaan. On myös tilanteita, joissa kampanjoiden on tärkeää pyrkiä pysymään näkymättömissä ja jäämään huomaamattomiksi, jolloin ihmiskäyttäjien soveltaminen on ehdottomasti paras, mutta myös kallein tapa. Tämä vaatii sekä osaavia käyttäjiä että merkittävämpiä resursseja tukemaan kampanjaa.

Toisaalta astroturffaus-kampanjoita voidaan käydä myös sosiaalisen median ulkopuolella. Merkittävä esimerkki digitaalisesta astroturffaus-kampanjasta sosiaalisen median ulkopuolella tapahtui osana internetin neutraaliuudesta käytävää keskustelua Yhdysvalloissa 2017. Federal Communications Comission (jatkossa tekstissä nimellä FCC. Liittovaltion virasto, joka valvoo muun muassa teleoperaattoreiden toimintaa) pyysi kansalaisilta kommentteja liittyen lainsäädännön tulkintaan. Kyseessä oli hyvin kiistanalainen muutos, sillä FCC halusi kumota presidentti Obaman kaudella vuonna 2015 säädetyn lain, joka määritti, että palveluntarjoajilla ei ole oikeutta rajoittaa tai sensuroida verkkosivuja, rajoittaa verkkonopeuksia erilaisille laillisille palveluille tai laskuttaa korkeampia hintoja myydäkseen niin sanottuja “etupasseja” internettiin. Muutosta tulkittiin laajasti askeleeksi vähemmän vapaata ja enemmän yritysten hallinnassa olevaa internettiä ja sen nähtiin erityisesti hyödyttävän teleoperaattoreita – kuluttajien kustannuksella.[195]

[194] Kovic, M., Rauchfleisch, A., Sele, M. & Caspar, C. 2018. Digital Astroturfing in politics: Definition, Typology, and Countermeasures. *Studies in Communication Sciences.* Vol 18. No.1
[195] https://slate.com/technology/2018/06/net-neutrality-is-officially-dead-heres-how-youll-notice-its-gone.html, https://www.theverge.com/2018/6/11/17439456/net-neutrality-dead-ajit-pai-fcc-internet, https://mashable.com/2018/04/23/net-neutrality-dead-explained/?europe=true

FCC keräsi lakimuutokseen liittyen noin 22 miljoonaa kommenttia. Tutkijat kuitenkin arvioivat, että näistä kommenteista jopa yli 90 % saattoi olla astroturffaus-kampanjan seurauksena generoituja. [196] Ne sisälsivät muun muassa samankaltaista kieltä ja ilmaisuja, ei-pysyviä tai kopioituja sähköpostiosoitteita, sekä näyttivät voimakkaita merkkejä siitä, että ne olivat automatisoiduilla tekstintuotto-ohjelmilla kirjoitettuja johtaen tutkijat vakavasti epäilemään niiden aitoutta. [197] Löydökset saivat jälkikäteen myös FCC:n johtajan myöntämään, että useat miljoonat kommentit eivät todennäköisesti olleet valideja. [198] Noin 500 00? kaikista kommenteista oli tullut venäläislähtöisistä sähköpostiosoitteista johtaen epäilyksiin osittaisesta venäläis-lähtöisesti sekaantumisesta.[199]

Esimerkkejä sosiaalisessa mediassa toteutetuista poliittisista astroturf-kampanjoista löytyy laajasti. Esimerkiksi vuonna 2012 Etelä-Korean presidentinvaalien alla paljastui laaja astroturf-kampanja, jota Etelä-Korean National Intelligence Service (NIS) oli ajanut noin kahden vuoden ajan. Tarkoituksena oli varmistaa konservatiivisen presidenttiehdokkaan, Geun-hye Parkin voitto presidentinvaaleissa. NIS:n toimijat olivat käyttäneet noin 1 500–3 500 ihmisvoimin ohjattua käyttäjää operaatiossa, jossa arviolta 30 eri tiimiä oli työskennellyt levittääkseen disinformaatiota ja julkaistakseen ehdokasta tukevia näkemyksiä.[200]

Astroturffaus onkin äärimmäisen laajalle levinnyt toimintamuoto. Jos se käsitetään laajimmassa määritelmässään, valheellisena ruohonjuuritason toimintana, suurin osa laskennallisesta propagandasta keskustelujen ja algoritmien manipulaatiosta voitaisiinkin laskea sen alle. Tästä ei kuitenkaan ole syntynyt selkeää yksimielisyyttä, minkä takia astroturffausta käytetään vähemmän sateenvarjoterminä ja useammin kuvaamaan tiettyä aspektia operaatioista muiden laskennallisen propagandan termien rinnalla.

---

[196] Hitlin, P., Olmstead, K. & Toor, S. 2017. *Public Comments to the Federal Communications Commission About Net Neutrality Contain Many Inaccuracies and Duplicates*. Pew Research Centre

[197] Ibid.

[198] https://fortune.com/2018/12/05/fcc-fraud-comments-chair-admits/

[199] Hitlin, P., Olmstead, K. & Toor, S. 2017. *Public Comments to the Federal Communications Commission About Net Neutrality Contain Many Inaccuracies and Duplicates*. Pew Research Centre., https://fortune.com/2018/12/05/fcc-fraud-comments-chair-admits/

[200] Keller, F. Schoch, D., Tier, S. & Yang, J., 2020. Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign. *Political Communication.* Vol 37. No. 2.
https://www.theguardian.com/world/2017/aug/04/south-koreas-spy-agency-admits-trying-rig-election-national-intelligence-service-2012

4.6. Poliittinen trollaus ja trollifarmit

Trollaus tai trollit ovat termejä, joita käytetään hyvin monessa yhteydessä, usein kuvaamaan jonkinlaisena sateenvarjo-terminä lähes kaikkia negatiivisia tai epäsopua luovia antisosiaalisia käytösmalleja internetissä. Se yhdistetään usein disinformaatiokampanjoihin, mielipiteen manipulointiin ja propagandaan, joissa usein puhutaan poliittisista trolleista ja poliittisesta trollauksesta.

Ongelmallista on, että lähteestä riippuen tietynlaiseen toimintaan osallistuva henkilö voidaan identifioida monella erilaisella termillä tai leimalla. Trollista voidaan puhua henkilönä joka 'pyrkii manipuloimaan mielipiteitä levittämällä huhuja, spekulaatiota tai väärää informaatiota'.[201] Toiset määritelmät painottavat voimakkaammin reaktion hakemista uhrilta, korostaen käytöstä, jossa trollit pyrkivät hajottamaan tai häiritsemään keskusteluja, ärsyttämään osapuolia sekä houkuttelemaan käyttäjiä turhiin argumentteihin, joiden tarkoitus on turhauttaa tai vihastuttaa osallistujia.[202]

Trollauksen ja trollien laaja käyttö terminä, epäselkeä terminologia ja liian laajasti käytetyt leimat, tekevät siitä vaikean määritellä tarkasti. Jotkut tutkijat määrittelevät trollauksen yksinkertaisesti puheeksi tai käytökseksi, jossa henkilöt esittävät rasistisia, fasistisia, vihapuhetta tai voimakasta seksismiä sisältäviä kommentteja. Laaja tutkimus islamofobiasta ja trolleista sosiaalisessa mediassa luokitteli trolleiksi käyttäjät, jotka julkaisivat islamofobisia tai ksenofobisia kommentteja tai vihapuhetta tai jakoivat tällaista sisältöä.[203] Puhuttaessa laajasti trolleista ja trollauksesta voidaan sanoa viitattavan lähes kaikkeen pahantahtoiseen, vahingolliseen tai vihamieliseen toimintaan. Jos se tapahtui, trollit todennäköisesti tekivät sen.

Ymmärtääkseen nykyaikaista poliittista trollausta, on kuitenkin tajuttava sen tarkoitusperä. Nykyaikainen verkossa ja sosiaalisessa mediassa nähtävä poliittinen trollaus kehittyi olomuotoonsa monien vuosien aikana. Trollaus ilmiönä on lähtöisin verkon aikasilta foorumeilta ja ensimmäisistä verkkopeleistä. Erilaiset alakulttuurit

[201] Mihaylov, T., Georgiev, G., & Nakov, P. 2015. Finding opinion manipulation trolls in news community forums. *Conference on Computational Natural Language Learning (CoNLL)*, K15-1032. p. 310–314.
[202] Mikolov, T., Sutskever, Ilya., Chen, K., Corrado, G., & Dean, J. 2013. Distributed representations of words and phrases and their compositionality. *Proceedings of the International Conference on Neural Information Processing Systems* (NIPS'13). P. 3111–3119.
[203] Pintak, L., Albright, J., Bowe, B. & Shaheen, P. 2020. *#Islamophobia: Stoking Fear and Prejudice in the 2018 Midterms*. *A multiplatform study of trolls: Social Media, Fringe Media, and the Real World*.

tunsivat trollit ilmiönä hyvin, sillä ne olivat läpäisevä osa verkkoa ja näin niistä tuli asia, jonka kanssa lähes jokaisen alakulttuuriin uppoutuneen oli elettävä. Tästä todennäköisesti lähtee myös alkuperäinen väärinymmärrys, joka vaivaa tulkintaa nykypäivän poliittisesta trollauksesta. Trollaus ymmärretään luonteeltaan hyvin reaktiohakuiseksi[204] ja yleensä nuorten esimerkiksi vaihtoehtoisoikeiston jäsenten harrastukseksi.[205]

Poliittisin trollauksen merkittävin tarkoitusperä ei kuitenkaan ole hakea reaktiota vaan hajottaa. Nykypäivän poliittiset trollit eivät pyri vakuuttamaan tai voittamaan vaan hajottamaan. Tarkoituksena ei välttämättä ole puskea tiettyä dialogia vaan sytyttää ristiriitoja ja hajottaa yhteisöjä. Venäjän 2016 koordinoimien Yhdysvallan presidentinvaaleihin liittyvien operaatioiden taustalla ei ollut yhtä voimakkaasti tietyn, yhtenäisen viestin läpivienti vaan yhteisöjen ja julkisen diskurssin hajottaminen. Tämä on myös trollien suurin vahvuus. Propagandabotteina tai disinformaation levittäjinä ne olisivat parhaimmillaan keskinkertaisia, jos niiden tarkoitus olisi vakuuttaa kuulijansa viestistään. Koska trollien ja trollauksen tarkoitus ei kuitenkaan strategisessa mielessä ole tehdä näin, vaan aiheuttaa kuulijoissaan hämmennystä, sekaannusta, sekä saada luopumaan diskurssista ja pyrkimyksistä siviiliin keskusteluun ja dialogiin. Trollit ovat vahvimpia, kun ne luovat kaaosta julkisessa diskurssissa ja juuri tämä on poliittisten trollien ja trollauksen pohjimmainen tarkoitus.

4.6.1. Trollifarmit ja valtiosponsoroitu trollaus

Trollifarmilla viitataan laajempaan, järjestäytyneeseen ja yhtenäiseen joukkoon. Trollifarmit keskittyvät disinformaatiotyön toteuttamiseen laajemmalla skaalalla ja niiden työ on tyypillisesti hyvin organisoitua. Trollifarmilla voi työskennellä tyypillisesti 10–500 työntekijää, jotka seuraavat säännöllisiä työvuoroja ja saavat selkeät ohjeet toimintaansa esimiehiltä. Joissakin tehtävissä ne pyrkivät täyttämään päivittäiset tuotantovaatimukset julkaisujen, kommenttien tai muun tuottavuusmittarin kautta. Palkat työntekijöille erityisesti vähemmän varakkaissa maissa voivat olla tavallisen kassatyön

[204] Malmgren, E. 2017. Don't Feed the Trolls. *Dissent.* Vol 62. No. 2., Binns, A., 2012. Don't Feed the Trolls! *Journalism Practice.* Vol 6. No 4
[205] Malmgren, E. 2017. Don't Feed the Trolls. *Dissent.* Vol 62. No. 2

verran, siis tyypillisesti minipalkan lähellä. Toisaalta osaaville työntekijöille haastavammissa tehtävissä voidaan maksaa merkittävästi enemmän.[206]

Ilmiöön on herätty myös tutkimuksen puolella. NATO STRATCOMin vuoden 2019 raportti tarkastelee trollifarmien toimintamalleja Filippiineillä, jossa se tunnistaa neljä erilaista toimintamuotoa, poliittisten kampanjoiden työntekijöistä yrityksiin ja valtiollisesti tuettuihin toimijoihin. Samalla raportti tunnistaa alan nousevana toimialana, jossa tyypilliset työntekijät tai toimijat ovat nuoria, menestyviä yrittäjiä, pyrkimyksenään myydä digitaalinen osaamisensa poliittisille kampanjoille ja yrityksille.[207]

Vuoden 2016 jälkeen eräs tunnetuimmista trollifarmeista on venäläinen IRA tai Internet Research Agency. Selvitys vuoden 2016 Yhdysvaltojen presidentinvaalien vaalihäirinnästä ja Trumpin yhteistyöstä venäläisten kanssa näytti Venäjän toiminnan keskittyneen tapahtumaan pitkälti IRA:n kautta.[208] Useat erilliset lähteet ovat vahvistaneet organisaation läheiset suhteet Venäjän valtioon.[209] (Luku 3.1 sisältää tarkempia kuvauksia IRA:n toiminnasta.)

4.7. Doxing

Doxing, suomeksi doksaus. Termi Doxing tulee ilmaisusta “dropping docs”, vapaasti suomennettuna dokumenttien julkaisu, joka tarkoittaa tunnistavan tai yksityisen informaation jakamista verkossa.[210]

Doksauksella viitataan henkilön yksityisten tietojen tarkoitukselliseen jakamiseen verkossa. Keräämällä henkilöstä yksityistä, tunnistettavaa tietoa hyökkääjät pyrkivät joko hiljentämään, pelottelemaan, uhkaamaan, nöyryyttämään, vahingoittamaan tai rankaisemaan henkilöä. Tieto henkilöstä voi olla joko vapaasti saatavissa mutta hankalassa muodossa olevaa informaatiota, jonka löytäminen ja yhteen kokoaminen voi

[206] https://www.occrp.org/en/investigations/inside-a-ukrainian-troll-farm, https://www.theguardian.com/world/2019/nov/01/undercover-reporter-reveals-life-in-a-polish-troll-farm,https://www.nytimes.com/2015/06/07/magazine/the-agency.html
[207] Ong, J. & Cabanes, J. 2019. *Politics and Profit in the Fake News Factory. Four Work Models of Political Trolling in the Philippines.* NATO STRATCOM COE.
[208] Special Counsel Robert S. Mueller. 2019. *Report on The Investigation Into Russian Interference in the 2016 Presidential Election. Volume I of II*. U.S. Department of Justice.
[209] Filipov, D. 2017, Oct 09. Shining a light on russian 'troll farm'. *The Washington Post*., https://www.voanews.com/europe/inside-internet-research-agency-mole-among-trolls
[210] https://www.wired.com/2014/03/doxing/

vaatia merkittävää vaivaa tai muuta tunnistetietoja. Tällainen tieto voi olla esimerkiksi julkisissa tietokannoissa tai rekistereissä tai se voi viitata vanhoihin sosiaalisen median julkaisuihin tai yrityksen taikka yhdistyksen internet-sivustoon. Vaihtoehtoisesti tieto voi olla hankittu esimerkiksi verkkohyökkäyksen eli hackin kautta tai hyödyntäen sosiaalisia menetelmiä (social engineering), jolloin tieto saadaan vapaaehtoisesti uhrilta, hänen työntekijöiltään tai perheenjäseniltä, joko manipuloimalla tai muuten harhaanjohtamalla heitä.

Doksaus on yleistynyt toimintamuotona sekä kulttuurisissa että sosiaalisissa taisteluissa ja myös politiikassa. Samalla journalisteihin kohdistuva doksaus on muuttunut arkipäiväisemmäksi. Esimerkiksi Luvussa 4.3 esitelty esimerkki Donald Trumpin kampanjan kokoamista dossieresta, tai tietokannoista on hyvä esimerkki journalistien sekä muiden näkyvien henkilöiden systemaattisesta, poliittisesti motivoidusta doksaamisesta. Tässä yhteydessä henkilöistä jaettava tieto ei välttämättä ole niinkään tunnistetieto, vaan sen tarkoituksena on löytää uhria vastaan käytettäviä yksityiskohtia hänen menneisyydestään, esimerkiksi hyökkäyksen laukaisemiseksi häntä kohtaan. Toisena esimerkkinä voitaisiin mainita Hillary Clintonin kampanjan sähköpostien vuoto edeltäen vuoden 2016 presidentinvaaleja. Tämä vuoto oli osa IRA:n monivuotisia vaikutusoperaatioita Yhdysvalloissa. (Katso luku 3.1)

Doksaus voi myös sisältää esimerkiksi yksilön kuten poliitikon tai muun julkkiksen osoite- ja yhteystietojen julkaisun (Tästä esimerkkinä 2018 tapahtunut välikohtaus, jossa vihastunut entinen työntekijä halusi kostaa esimiehelleen sekä neljälle muulle republikaanipoliitikolle, jotka olivat tukeneet Brett Kavanaughin valintaa korkeimman oikeuden tuomariksi, jolloin henkilö päätyi jakamaan näiden henkilökohtaiset tiedot verkkoon[211]), perheen tietojen tai lasten koulupaikan julkaisemisen.

Vuonna 2015 nousseessa tapauksessa hyökkääjät yrittivät kiristää avioliitossa oleville henkilöille suunnattua seuranhakusivustoa, Ashley Madisonia, uhkaamalla julkaisevansa tietokannan sivuston käyttäjistä. Hyökkääjät toteuttivat uhkauksensa, joka johti noin 30 miljoonan käyttäjän tietojen vuotamiseen. Paljastuneiden tietojen seassa oli julkisuuden henkilöiden, virkamiesten, poliitikkojen, kirkon viranomaisten sekä monien muiden

[211] https://www.npr.org/2019/10/29/774386731/former-senate-aide-gets-probation-for-helping-dox-republicans-over-kavanaugh-hea?t=1600773040077

yhteystietoja. Vuoto johti lukuisiin irtisanomisiin, eroamisiin työpaikoista, itsemurhiin ja avioeroihin.[212]

Lopuksi doksaamista on käytetty myös sosiaalisen oikeuden keinona. Vuonna 2017 Yhdysvaltoissa Charlottevillessä tapahtuneisiin "valkoisen ylivallan" (white supremacy) protesteihin osallistuneiden kuvia ja henkilötietoja päädyttiin levittämään sosiaalisessa mediassa. Eräs uhreista, Joey Saladino, joka oli protestien aikaan ollut toisessa maassa, kertoi, miten hänet oli sosiaalisessa mediassa (väärin) tunnistettu erääksi osallistujista. Uutisen levitessä sosiaalisessa mediassa, hän joutui altistumaan hyökkäyksille, kuolemanuhkauksille ja häirinnälle.

Esimerkkien on tarkoitus havainnollistaa erityisesti sosiaalisen median voimaa doksauksen kontekstissa. Doksauksesta vaarallista ja tehokasta ei välttämättä tee vain se, että henkilö ei haluaisi tietoja julkaistavan. Doksaus itsessään voi johtaa voimakkaaseen, yksilöön kohdistuvaan vihareaktioon vuotaneiden tietojen seurauksena ja aiheuttaa jopa skandaaleja, mikäli tiedot itse ovat olleet riittävän arkaluontoisia.

4.8. DDoS-hyökkäykset

DDoS-hyökkäys on eräs suorimmista laskennallisen propagandan muodoista. Se tarkoittaa verkkohyökkäystä käyttäen tyypillisesti bottiverkkoa, jossa tarkoitus on hyödyntää verkkosivun tai palvelimen heikkoutta ja ylikuormittaa ja kaataa verkkosivu.[213] Tarkoituksena on tyypillisesti lamauttaa verkkopalvelu tai sivusto strategisesti tärkeään aikaan ja pitää se poissa käytöstä tietyn ajan. Motiiveina voi olla palvelun häiritseminen, poliittisen kilpakumppanin torjunta tai yhteiskunnallisesti tärkeiden infrastruktuurien tai palveluiden esto tai horjuttaminen.

DDoS-hyökkäyksillä häirittiin esimerkiksi Yhdysvaltain 2018 presidentinvaalien kampanjointia, jolloin tunnistamattomat hyökkääjät kohdistivat DDoS-hyökkäyksen demokraattisen kampanjan verkkosivustoihin heinäkuussa 2018. Hyökkäykset kohdistuivat sivustoihin strategisesti kriittisiin aikoihin pyrkien yhdessä tapauksessa

[212] https://www.theguardian.com/technology/2016/feb/28/what-happened-after-ashley-madison-was-hacked
[213] Bentzen, N., 2018. *Computational Propaganda Techniques*. European Parliamentary Research Service (ERPS)., https://www.digitalattackmap.com/understanding-ddos/

hankaloittamaan varainkeruuta ja iskien toisessa verkkosivun saadessa merkittävää julkisuusnäkyvyyttä.[214]

Toisena esimerkkinä ovat Viroon vuonna 2007 kohdistuneet kyberhyökkäykset, jotka alkoivat entisen Neuvostoliiton sotamonumentin siirtämisestä. Tämä johti laaja-alaisiin hyökkäyksiin, joissa koordinoidut DDoS-iskut pysäyttivät lähes koko maan verkkopalvelujen toiminnan useiksi viikoiksi. Iskut kohdistuivat valtion virastoihin, pankkeihin, teleoperaattoreihin ja internetin tarjoajiin, mediataloihin sekä pienyrittäjiin. Iskun seurauksena pankkiautomaatit ja verkkopankit toimivat viikkojen ajan vain satunnaisesti. Virastojen sisäinen viestintä, yhteydet ja sähköpostit lakkasivat toimimasta tai katkeilivat, uutissivustot ja -lähetykset eivät pystyneet toimittamaan uutisia, verkko- ja puhelinyhteydet kokivat katkoja. Viro itse syytti iskuista Venäjää.[215] NATOn STRATCOM raportti, joka arvioi iskuja, totesi merkittävän määrän hyökkäykseen liittyneistä yhteyksistä tulleen Venäjältä. Raportti myös nosti esille, että hyökkäyksiä edelsi ja reunusti merkittävä määrä vihamielistä retoriikkaa, Viron kannalta epäsuotuisia taloustoimia sekä täysi kieltäytyminen osallistumisesta iskujen tutkimiseen näiden jälkeen.[216] Venäjä kuitenkin kielsi osallisuutensa iskuihin. [217]

Venäjä käytti DDoS-hyökkäyksiä myös osana pitkäaikaisia vaikutusoperaatioitaan Yhdysvalloissa (katso luku 3.1), jossa Venäjän tiedustelupalvelu GRU suoritti kohdennettuja hyökkäyksiä muun muassa DNC:n (Democratic National Committeen) sekä kriittiseen äänestysinfrastruktuuriin. Onnistunut hyökkäys DNC:tä kohtaan johti myös yhteen merkittävimmistä tietovuodoista silloisen presidenttiehdokas Clintonin sähköpostien vuotaessa julkisuuteen IRA:n Wikileaks-sivustolle jakamana.

4.9. Massaviestikampanjat

Uudehko, toistaiseksi vain Yhdysvaltojen poliittisessa kontekstissa esiintynyt vaalikampanjoinnin menetelmä ovat massa-tekstiviestikampanjat, jotka kiertävät lakeja suorista yhteydenotoista ja hyödyntävät kampanjoiden keräämiä valmiita tietokantoja.[218]

[214] https://www.cyberscoop.com/ddos-democratic-campaigns-primary-dnc-dccc/
[215] https://www.bbc.com/news/39655415
[216] NATO STRATCOM COE. 2007. *2007 Cyber Attacks on Estonia*.
[217] https://www.baltictimes.com/news/articles/17908/
[218] https://www.fastcompany.com/90469445/inside-the-2020-campaign-messaging-war-thats-pelting-our-phones-with-texts

Osittain menetelmä nojaa uuden ja vanhan teknologian yhdistelmään. Yhdysvalloissa liittovaltiolaki vaatii poliittisia kampanjoita pyytämään suostumuksen ennen tekstiviestien lähettämistä äänestäjille. Uudet rinnakkaisviestintäalustat (peer-to-peer platforms) hyödyntävät laillista porsaanreikää, joka sallii yksittäisten viestien lähettämisen äänestäjille, mutta kieltää automatisoidut massaviestit.[219] Rinnakkaisviestintä-alustat käyttävät kampanjoiden vapaaehtoisia tai palkattuja työntekijöitä, jotka lähettävät viestejä potentiaalisille äänestäjille.[220]

Toiminta on hitaampaa kuin automatisoitujen viestien lähettäminen, mutta se on laillista ja viestimuotona äärimmäisen tehokasta. Alexander Ocasio Cortezin valintakampanja lähetti noin 120 000 viestiä osana valintakampanjaansa.[221] Osana 2018 Yhdysvaltain kongressivaaleja, eri poliittisten toimijoiden arvioitiin lähettäneen noin 100 miljoonaa tekstiviestiä.[222] Donald Trumpin kampanja on ilmoittanut tähtäävänsä miljardiin tekstiviestiin osana 2020 presidentinvaalikampanjaa.[223]

Kampanjat käyttävät rinnakkaistekstausta muun muassa vapaaehtoisten rekrytoimiseen, lahjoitusten keräämiseen sekä potentiaalisten äänestäjien aktivoimiseen ja paikantamiseen.[224] Osa sen tehosta tulee muun muassa siitä, että tekstiviestit viestintämuotona tavoittavat vastaanottajansa merkittävästi tehokkaammin palveluja tarjoavien yritysten mukaan. Nämä palvelut väittävät saavuttavansa jopa yli 90% luetuksitulemisen.[225]

Massatekstausta on käytetty myös osana laittomia kampanjoita. Vuonna 2018 kaksi republikaanipoliitikkoa joutui laaja-alaisen tekstiviestien kautta toteutetun

[219] Ibid.
[220] https://medium.com/political-moneyball/how-p2p-texting-is-revolutionizing-politics-bfe697c2abb8
[221] https://www.vice.com/en_us/article/vbjjw9/text-campaigns-are-changing-american-politics-and-nobodys-ready
[222] Ibid.
[223] https://www.fastcompany.com/90502877/5-things-to-consider-if-you-want-to-reimagine-your-career-for-an-uncertain-future
[224] Ibid.
[225] https://www.hustle.com/how-it-works/., https://www.getthru.io/

loanheittokampanjan kohteeksi Tennesseen osavaltiossa, jotka käyttivät samantyylisiä viestejä ja viestintää kuin rinnakkaisviestintäkampanjat.[226]

4.10. Sosiaalisen median mainonta ja mikrokohdennus

Luvussa viimeisenä käsitellään hyvin keskeinen laskennallisen propagandan keino, mikrokohdennettu mainonta. Mikrokohdennettu mainonta viittaa tyypillisesti sosiaalisessa mediassa esiintyvään, hyvin tarkasti kohdennettuun data-painotteiseen mainonnan muotoon. Vaikka sosiaalisessa mediassa tapahtuvaa mainontaa ei alun perin mielletty laskennalliseksi propagandaksi, asenteet sekä tutkijoiden että julkisuuden henkilöiden keskuudessa ovat muuttuneet voimakkaasti viimeisten vuosien aikana. Merkittävät yksityisyyden, tietovuotojen ja epäselvien vaalisekaannusten kriisit kuten Cambridge Analytica ovat siirtäneet huomiota sosiaalisen median mainontaa kohtaan yhä voimakkaammin. Facebookin vahva kanta antaa poliitikkojen puhua mainoksissaan ilman rajoituksia tai sensuuria on johtanut tilanteeseen, jossa mainosten sisältöä sosiaalisessa mediassa hyvin harvoin kyseenalaistetaan tai valvotaan. Samalla tehokkaammat sisällön optimointimenetelmät ovat johtaneet mainonnan kohdalla tilanteeseen, jossa sisällön merkitys vaikuttavuuden verrattuna on entistä pienempi.

Mikrokohdennus tarkoittaa hyvin kohdennettujen, testattujen ja yksilöityjen mainosten toimittamista suppealle kategorialle äänestäjiä,[227] käyttäen dataa ja data-analyysiä, joka on kerätty yksilön tunnistuspiirteistä, kuten kulutus-, elämäntyyli- ja verkkokäyttäytymistavoista.[228] Tarkennusta saatetaan usein edistää yhdistelemällä monia erillisiä tietokantoja, jonka lisäksi jotkin yritykset käyttävät toimintansa tukena psykometristä profilointia muodostaakseen entistä tarkempia segmenttejä ja profiileja. Sosiaalisen median mainonnan rooli on ollut kyseenalaisena myös ulkomaisten vaikutusoperaatioiden yhteydessä ja sen roolia pohdittiin merkittävästi Yhdysvaltain senaatin tutkimuksissa Venäjän sekaantumisesta 2016 presidentinvaaleihin. Vaikka Venäjän toimijat olivat käyttäneet jonkinasteisia summia sivustojensa sekä julkaisujensa kattavuuden kasvattamiseen (mainoksiin käytettiin enimmillään yhteensä noin 100 000

[226] https://medium.com/political-moneyball/how-p2p-texting-is-revolutionizing-politics-bfe697c2abb8., https://www.vice.com/en_us/article/vbjjw9/text-campaigns-are-changing-american-politics-and-nobodys-ready
[227] W. Gorton. 2016. Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy. *New Political Science*. Vol 37. no. 1
[228] Rubinstein, I. 2014. Voter Privacy in the Age of Big Data. *Wisconsin Law Review*. No 5.

dollaria)[229], ei sen rooli ole ollut niin huomattava vieraiden toimijoiden vaikutusoperaatioiden yhteydessä. Tätä voi selittää joko se, että nämä toimijat valitsevat luoda näkyvyytensä orgaanisen kasvun kautta, tai se, että ne mieluummin sijoittavat resurssinsa muihin mahdollisuuksiin.

Alue, jossa sosiaalisen median mikrokohdennettu mainonta on saanut merkittävästi suurempaa jalansijaa, on ollut perinteinen poliittinen kampanjointi erityisesti Yhdysvalloissa. Muun muassa Donald Trumpin presidenttikampanjan markkinointipäällikkö Brad Parscale on puhunut julkisesti mikrokohdennuksen eduista. Hän väitti jopa, että se oli syy Trumpin voittoon 2016. Parscale kertoo, että yhdessä Facebookin teknisen tuen (Facebook tarjoaa huomattaville mainostajille ilmaista konsultointia ja teknistä tukea mainonnassa lähettämällä henkilöstöä konsultoimaan kampanjan juoksuttamisessa ja mainonnassa Facebookin kautta[230]) tehokkaan mikrokohdennuksen ja A/B-testauksen kautta he pystyivät toimittamaan ja testaamaan keskimäärin 50–60 000 erilaista mainosta päivittäin, kohdistettuna satojen tai vain kymmenten äänestäjien mikrosegmenteille.[231]

Samalla sosiaalisen median mainonta on merkittävästi kustannustehokkaampaa. Siinä missä perinteinen mainonta on usein vaihtokauppa kohdennuksen ja kattavuuden välillä, sosiaalisen median mainonta mahdollistaa sekä äärimmäisen tarkan kohdennuksen että kattavuuden. Perinteinen mainonta esimerkiksi printtimediassa, televisioissa tai tienvarsilla antoi mainostajan tyypillisesti kohdentaa mainoksen enintään maantieteelliseen alueeseen, lehden lukijakuntaan tai tietyn ohjelman katsojiin. Toisaalta prosessi oli kohtalaisen edullinen, mutta sen tarkkuus ei ollut lähelläkään toivottua tasoa. Henkilökohtaisesti postitetut vaalimainokset tarjosivat tarkennuksen suhteen oman etunsa mahdollistaen kohdennuksen yksilötasolla niin pitkälle kuin oli toivottavaa. Tämä toimitustapa oli kuitenkin merkittävästi työintensiivisempi ja kalliimpi eikä sisältänyt esimerkiksi printtimedian tai TV:n kustannustehokasta saavuttavuutta.

---

[229] Howard, P., Ganesh, B., Dimitra, L., Kelly, J.& Francois, C., 2018. *The IRA, Social Media and Political Polarization in the United States, 2012-2018.* Computational Propaganda Research Project.
[230] https://www.cbsnews.com/news/facebook-embeds-russia-and-the-trump-campaigns-secret-weapon/
[231] Parscale viittaa kohdennettuun optimointiin ja testaukseen, jossa mainosten vaikuttavuutta seurataan välittömästi sosiaalisessa mediassa. Parscalen mukaan tämä mahdollisti sen, että kampanja pystyi toimittamaan päivässä kymmeniä tai satoja tuhansia erilaisia mainoksia, jotka kaikki erosivat toisistaan hyvin pienillä tavoilla, löytääkseen parhaiten toimivat variaatiot. Erot mainosten välillä saattoivat koostua esimerkiksi eroavasta sanamuodosta, väristä, asettelusta tai vastaavista seikoista, säilyttäen usein kuitenkin saman viestin.

Verkossa tehtävä mikrokohdistettu sosiaalisen median mainonta puolestaan mahdollistaa kustannustehokkaan, edullisen ja todella hyvin kohdennetun mainonnan muodon, joka voi myös saavuttaa sellaisia äänestäjiä, joita perinteiset markkinointikeinot eivät välttämättä ole aiemmin tavoittaneet. Ja koska segmentit voivat olla hyvin pieniä, on mainokset mahdollista kohdistaa niille segmenteille, jotka kaikkein todennäköisimmin välittävät niistä tai kokevat kyseisen asiakysymyksen itselleen tärkeäksi.

4.11. Yhteenveto

Laskennallinen propaganda ei rajoitu vain sosiaaliseen mediaan tai sisällön tai käyttäjien manipulointiin. Se on äärimmäisen monipuolinen ilmiö, joka sisältää mainonnan, sisällöntuotannon ja luomisen, valetilien ja -sivustojen käytön, botit, kehittyneet- ja hybridibotit, vahingollisen käytöksen ja hyökkäykset käyttäjien kimppuun, hyökkäykset infrastruktuuriin tai automatisoidun ylläpidon hyväksi käyttämisen, lainsäädännölliset porsaanreiät ja algoritmisen manipulaation, psykometriikan ja persoonallisuusprofiloinnin. Jokaisella kuvatusta menetelmästä on mahdollisuus saada aikaan merkittäviä vaikutuksia osana suurempaa kampanjaa. Oikealla tavalla kohdistettuna kriittiseen paikkaan ja aikaan oikea tai kenties väärä toimija voi saada aikaan hyvin merkittäviä vaikutuksia. Kaikki keinot eivät ole vain valtiollisten toimijoiden käyttämiä ja myös poliittiset puolueet ovat pelissä mukana, etsien kilpailuetuja kannatuksensa kasvattamiseksi ja menestyksensä parantamiseksi.

Yhdysvaltojen kaksipuoluejärjestelmä, poliittisten puolueiden merkittävät resurssit sekä toimijoiden korkea tekninen osaaminen onkin johtanut tilanteeseen, joissa poliittiset toimijat Yhdysvalloissa ajavat omalla tavallaan laskennallisen propagandan innovointia. Vaikka näiden toimijoiden motiivit ovat yleensä vähemmän pahantahtoisia kuin esimerkiksi valtiollisten, ovat ne toisaalta johtaneet myös poikkeuksellisen kyseenalaisiin innovaatioihin, kuten potemkin-uutissivustoihin pink-slime uutisointiin, jolla tulee varmasti lähivuosina olemaan oma merkityksensä ilmiön yleistyessä ja tekoälyn luonnollisen kielen prosessoinnin kykyjen parantuessa.

Luku kuitenkin selkeyttää myös sitä, että olemme saapuneet tilanteeseen, jossa tarve pelisäännöille ja lainsäädännölle sosiaalisessa mediassa on vakava ja todellinen. Esimerkiksi amplifikaatio, astroturffaus ja verkkohyökkäykset yksilöitä kohtaan on

kielletty palveluiden käyttöehdoissa, mutta ne eivät ole rikoksia eikä niistä seuraa sanktioita, lukuun ottamatta kenties sosiaalisen median rikkeeseen syyllistyneen käyttäjätilin poistoa. Koska uuden luominen vie toisaalta alle 5 minuuttia, tätä ei voida pitää merkittävänä esteenä.

Jos siis mikään ei estä, kiellä tai rankaise ketä tahansa yksilöä käyttämästä laskennallisen propagandan keinoja omaksi edukseen, mikä säätelee yksilöiden käytöstä verkossa? Toisaalta tämä johtaa laajempaan kysymykseen siitä, miksi hyväksymme verkossa asioita, jotka todellisessa maailmassa eivät olisi hyväksyttäviä. On selvää, että tarvitsemme eri pelisäännöt virtuaalisen ja fyysisen todellisuuden välille, sillä ne seuraavat fundamentaalisesti erilaisia sääntöjä. Toisaalta käsityksemme etiikasta ja moraalista säilyvät pitkälti samanlaisina. Jos ideamme siitä, mikä on hyväksyttävää verkossa, vastaavat niitä, jotka ovat hyväksyttäviä jokapäiväisessä elämässämme, miksi emme asettaisi voimaan näitä samoja sääntöjä verkkoon, ainakin niiltä osin kuin se on järkevää.

Vaikka tämä ei yksin riitäkään ratkaisemaan ongelmaa, se olisi alku. Samalla voisimme tarkastella harmillista verkkokäyttäytymistä laajemmin ja puuttua myös siihen. Keskeistä kuitenkin olisi, että sosiaalinen media ei voisi enää 2020-luvulla säilyä villinä läntenä. Sosiaalisen median levinneisyys, erityisesti länsimaissa, velvoittaa meitä puuttumaan tilanteeseen ja suojelemaan yksilöitä heidän viettäessään aikaa verkossa.

Toisaalta voidaan myös selkeästi huomata, että osana ongelmaa on sukupolvinen jakaantuminen, joka on johtanut tilanteeseen, jossa vanhempien sukupolvien jäsenet eivät välttämättä tunne tai ymmärrä sosiaalisen median toimintaympäristöjä tai sen alustoja ja ongelmia yhtä hyvin. Sillä on selkeitä heijastuksia myös lainsäädäntöprosessiin, jossa itse lainsäädäntö toistaiseksi roikkuu hiukan perässä. Tämä on, yhdessä lainsäädäntöprosessin tyypillisesti hitaan ja kankean luonteen vuoksi, pitkälti johtanut tilanteeseen, jossa hyperkehittyvä sosiaalisen median toimintaympäristö on täysin onnistunut ohittamaan ja välttämään lainsäädännön ja säätelyn. Vaikka tämä sukupolvinen jakauma ei yksin ole selitys nykytilalle, se on ehdoton osa sitä.

Toinen, keskeisempi osa, on kuitenkin kysymys siitä, kenelle vastuu loppujen lopuksi kuuluu. Tähän vastaa työn viimeinen luku, luku 5.

5. Johtopäätökset ja toimenpide-ehdotukset

Lähtiessäni tekemään työtä laskennallisesta propagandasta ilmiönä oletukseni työn suhteen olivat jossain määrin erilaiset. Merkittävä osuus tutkimuksesta korostaa laskennallisen propagandan levinneisyyttä ja valtioiden sekä pahantahtoisten toimijoiden roolia sen levittäjänä (katso esimerkiksi Bradshaw & Howard, Cyber Troop Report 2019[232]). Oletin myös oman työni päätyvän jossain määrin vastaaviin lopputuloksiin kuvauksen ja tutkiskelun kautta.

Tässä suhteessa olin kuitenkin yllättynyt. Mitä enemmän olen tutustunut aiheeseeni ja jatkanut työni kanssa työskentelemistä, sitä enemmän olen päätynyt erilaiseen johtopäätökseen: *Alustat ovat ongelma*. Facebookin loppumaton tarve kumarrella autoritaarisia johtajia ja suojella pahantahtoisia toimijoita sekä olla puuttumatta ilmiöön ovat vain pieni osa tätä ongelmaa. Sosiaalisen median alustat itse ovat fundamentaalisesti suunniteltuja tavalla, joka rohkaisee disinformaation leviämistä ja jakamista sekä tarjoaa ihmisyyden rumimmille puolille keinon tulla amplifioiduksi moninkertaisesti. Samalla nämä puolet tekevät siitä suitsematta tai säätelemättä erityisen vaarallisen.

Se on tarjonnut toimijoille, kuten Venäjälle ja Kiinalle, tavan edistää niiden ulkomaisia etuja keinoin, jotka loukkaavat vieraiden valtioiden koskemattomuutta ja ovat esimerkki uudesta informaatiosodankäynnin muodosta, vaikka ne eivät nykyisen käsityksen mukaan ylitä traditionaalisen sodankäynnin tai loukkauksien kynnystä. Samalla niiden asettaminen vastuuseen on toistaiseksi, ei vain teknologian vaan myös Facebookin takia, äärimmäisen haastavaa. Koska laskennallisen propagandan ja disinformaation laajempia vaikutuksia ei tunneta, on helppo kyseenalaistaa sen merkitys ja vahingollisuus. Harvat valtiot haluaisivat katkaista diplomaattisia tai kauppasuhteita epäselvien informaatiotilassa tehtyjen toimien vuoksi. Vielä harvemmat olisivat valmiita vastaamaan aseellisin toimin. Kansainvälisten sanktioiden asettaminen ylikansallisten toimielinten kautta ei vielä ole mahdollista. Esimerkiksi WHO on ollut varovainen sen suhteen, ettei se nimeä toimijoita tai valtioita tai edes suoraan viittaa disinformaatioon puhuessaan koronavirukseen liittyvästä infodemiasta.[233]

---

[232] Bradshaw, S. & Howard, P. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. Computational* Propaganda Research Project.

[233] Mm. https://www.who.int/news-room/feature-stories/detail/immunizing-the-public-against-misinformation., https://www.who.int/news-room/feature-stories/detail/countering-misinformation-about-covid-19

Samalla kuitenkin kansainvälisten elinten tuomio pahimpia disinformaation levittäjiä kohtaan olisi voimakas toimi, joka tuomitsisi valtiot, jotka pyrkivät ajamaan omaa etuaan globaalin kriisin keskellä tai loukkaavat vieraiden valtioiden koskemattomuutta vaalivaikuttamisen kautta (kuten kappaleissa 3.1 ja 3.2). Ei ole epäilystäkään siitä, että Venäjä ja Kiina kieltäisivät syytökset jopa ylitsevuotavan todistusaineiston edessä (kuten ne ovat tehneet tähänkin asti[234]). Toisaalta Venäjän ja Kiinan toistuvat, selkeät linkit disinformaatio- ja vaikutuskampanjoihin lukuisissa maissa ovat kiistämätöntä todistusaineistoa niiden roolista ja osasta disinformaatiokampanjoita aktiivisesti toteuttavina toimijoina.[235] Tässä vaiheessa niiden kiellot asian suhteen tosin yhtä uskottavia kuin käsi keksipurkilla kiinni jääneen neljävuotiaan, hänen vaakuttaessaan, ettei ole syönyt tai edes aikonut syödä yhtään keksiä (eikä kekseistä puheenollen oikeastaan edes tiedä mistä puhut..)

Ja kuten esimerkiksi Luku 3.1 näyttää, kyse ei ole pienistä, muutaman kuukauden tai ehkä vuoden kestävästä huonosti suunnitellusta projektista moniongelmaista kehittyvää valtiota vastaan, vaan laajasti resursoidusta ja rahoitetusta monivuotisesta disinformaatio-operaatiosta, jota toteutetaan yhteistyössä useiden eri hankkeiden ja viranomaisten kautta (esimerkiksi GRU:n hyökkäykset vaali-infrastruktuuria kohtaan ja sen tietomurto DNC:n keskusjärjestöön ja näiden dokumenttien myöhempi julkaisu yhteistyössä IRA:n operaation kanssa) hyödyntäen äärimmäisen kehittynyttä ymmärrystä sosiaalisen median toimintaperiaatteista, amerikkalaisen yhteiskunnan rakenteesta ja sosiaalisista ongelmista sekä tuntemusta toimintakulttuurista ja kulttuurisista eroista. Lähes kaikki seikat Venäjän operaatiossa kuvasivat hyvää tuntemusta, korkeaa valmistelun tasoa ja kehittyneitä

[234] https://www.latimes.com/world-nation/story/2020-07-29/us-jabs-russia-over-claim-of-spreading-virus-disinformation, https://www.cnbc.com/2020/04/27/china-denies-spreading-coronavirus-disinformation-following-eu-report.html

[235] Bolsover, G. An Alternative Model of a Widespread Practice. Teoksessa Woolley, S. & Howard, P. 2019. *Computational propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. New York: Oxford University Press., Bradshaw, S. & Howard, P. 2019. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation.* Computational Propaganda Research Project., https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf., https://www.nytimes.com/2019/01/31/technology/twitter-disinformation-united-states-russia.html., https://misinforeview.hks.harvard.edu/article/pandemics-propaganda-how-chinese-state-media-creates-and-propagates-ccp-coronavirus-narratives/., https://www.aspistrategist.org.au/china-joins-the-global-disinformation-order/.

kompetensseja, jotka on saavutettu monivuotisen kokemuksen kautta. Samalla laajojen seurantakantojen kerääminen ilman merkittävää mainostusta tai taloudellisten resurssien sijoittamista voimistaa käsitystä taitavasta operaatiosta ja hienostuneesta toimijasta.

Keskeistä kuitenkin on, että kaikkien näiden operaatioiden toteuttaminen olisi mahdotonta ilman *sosiaalisen median alustojen implisiittistä* suostumusta antaa pahantahtoisten toimijoiden olla aktiivisia alustallaan. Esimerkiksi Facebookilla kesti noin 18 kuukautta siitä, kun se tuli tietoiseksi IRA:n operaatiosta alustallaan siihen, että se lopulta poisti operaatioon liitetyt tilit.

Tuorein ja eräs kauheimmista esimerkeistä siitä, miten Facebookin ja Googlen kaltaiset toimijat voivat suojella pahantahtoisia toimijoita, tulee Myanmarin kansanmurhasta vuodelta 2017. YK:n tarkkailijat kertoivat raportissa Facebookin roolin olleen keskeinen, muodostaen merkittävän osan konfliktia ja sen osana tapahtuneita hirveyksiä.[236] Keskeinen osa tätä olivat noin 500 sivun, 160 käyttäjän ja 17 ryhmän kokonaisuudet, jotka olivat olleet osa Myanmarin armeijan disinformaatiokampanjaa Rohingyan vähemmistöä kohtaan. Myöhemmin, Facebook poisti tilit alustaltaan koordinoidun epäautenttisen käytöksen takia, tosin ei ennen kuin pahin oli jo ehtinyt tapahtua. Sivustot olivat näennäisesti itsenäisiä uutissivustoja, viihde-, kauneus- ja elämäntyylisivuja, muistuttaen tässä suhteessa jossain määrin esimerkiksi Venäjän operaatioita Yhdysvalloissa, luvussa 3.1 (erityisesti niiden käyttämien valesivustojen kautta.) Poistetut sivustot olivat julkaisseet armeijan propagandaa ja etnisesti motivoituneeseen väkivaltaan rohkaisevia sisältöjä. Sivuilla oli kokonaisuudessaan noin 12 miljoonaa seuraajaa.[237]

Huolimatta näistä tapahtumista ja sen laajemmasta historiasta, Facebook ei ole valmis muuttamaan käytöstään. Kesäkuussa 2020, Gambian valtio asetti vireille haasteen Yhdysvaltain liittovaltio-oikeudessa saadakseen pääsyn Facebookin todistusaineistoihin Myanmarin tapahtumista. Gambia hakee todistusaineistoa osaksi Myanmaria vastaan käytävää oikeudenkäyntiä Kansainvälisessä tuomioistuimessa, jossa Facebookin

[236] United Nations Human Rights Council. 2018. *Fact-Finding Mission on Myanmar: Concrete and Overwhelming Information points to International Crimes*. United Nations.
[237] https://about.fb.com/news/2018/08/removing-myanmar-officials/., https://time.com/5197039/un-facebook-myanmar-rohingya-violence

dokumentit voisivat toimia todistusaineistona Myanmaria vastaan Kansainvälisen tuomioistuimen tutkinnassa Myanmarin kansanmurhan tapahtumista. Reaktiona Gambian haasteeseen, Facebook julkaisi vastauksensa, jossa se kyseenalaistaa Gambian vaatimukset ja vastustaa tietojen jakamista sanoen, ettei se halua asettaa vaarallista esimerkkiä ja että sille olisi ”raskasta” jakaa dataa tileistä, jotka se on jo poistanut ja arkistoinut.[238]

Facebook on säilyttänyt datan tapahtumiin ja niihin liitettyihin tileihin liittyen. Ei ole täysin selkeää, miksi Facebook kieltäytyy jakamasta dataa, jota voitaisiin käyttää todistusaineistona Myanmaria vastaan tutkinnassa ja oikeudenkäynnistä mahdollisesta kansanmurhasta. Jos uskomme Facebookin omia sanoja, vastaus voi olla, että se ei yksinkertaisesti välitä etnistä ryhmää kohtaan tapahtuvasta kansanmurhasta niin paljon, että se haluaisi jakaa todistusaineistonsa prosessin ollessa sille liian ”raskas”. Toiminta on kuitenkin voimakkaasti linjassa Facebookin historian kanssa sen toistuvasti kieltäytyessä lähes kaikista paitsi kaikkein paikoittavimmista pyynnöistä.[239]

Hyvin samanlainen, joskaan ei yhtä vakava esimerkki, ovat Googlen toimet Yhdysvaltain senaatin tutkinnassa Venäjän vaalisekaantumisesta luvussa 3.1. Siinä hyvin merkittävä osuus Googlen jakamasta datasta Yhdysvaltain senaatille ja sen tutkijoille oli joko täysin käyttökelvotonta, aiheeseen liittymätöntä, tahallisesti vaikeassa muodossa toimitettua ja sisältäen useita duplikaattitiedostoja.

Pohdittaessa siis itse ilmiötä alustojen rooli korostuu jatkuvasti. Facebookin kaltaiset alustat eivät vain mahdollista vihapuheen, vainon ja jopa kansanmurhien kaltaisten tapahtumien toteutumista uudella tavalla. Ne myös suojelevat tekijöitä seurauksilta ja varmistavat, ettei todistusaineisto jälkikäteen ole kenenkään muun kuin niiden itsensä saatavilla. Tähän rinnastettuna Facebookin oma argumentti siitä, että se kykenee olemaan vastuullinen ja samalla itseään säätelevä toimija, vaikuttaa jatkuvasti heikommalta.

Samaan aikaan ei myöskään ole kyse siitä, etteivätkö alustat *kykenisi* tarttumaan toimeen asioiden parantamiseksi. Vaikka jotkut ovat puolustaneet esimerkiksi Facebookia sanoen

[238] https://time.com/5880118/myanmar-rohingya-genocide-facebook-gambia/
[239] Pakoittavalla tarkoittaen että siitä kieltäytyminen olisi mahdotonta. Lähde: Ibid.

sen olevan liian suuri moderoitavaksi, todellisuus on, että Facebookin omat toimet ovat olleet lähes täysin riittämättömiä saavuttaakseen merkittäviä seurauksia.[240] Tällä hetkellä Facebook työllistää 15 000 sisältömoderaattoria.[241] Suhteutettuna 2.6 miljardiin kuukausittaiseen aktiiviseen käyttäjään tämä tarkoittaa, että jokainen sisältömoderaattori vastaa yksin yli 170 000 kuukausittaisen käyttäjän tuottamasta sisällöstä. Samaan aikaan Facebook on tarjolla 111 kielellä sen käyttäjien puhuessa ja tuottaessa sisältöä vielä useammilla kielillä.[242]

Edellä kuvattuun suhteutettuna Facebookin 15 000 henkilön sisältömoderaattori-tiimi on surullisen pieni. Samalla se voisi helposti korjata asioita. Esimerkiksi 15 dollarin tuntipalkalla, jonka Facebook maksaa työntekijöilleen (joista suurin osa työskentelee erillissopimuksella, joka ei oikeuta heitä täyden työntekijän etuihin, esimerkiksi terveysvakuutukseen tai muihin kompensaatioihin), se voisi helposti kolminkertaistaa sisältömoderaattori-tiiminsä koon.[243] Nykyisillä kustannuksilla tämä maksaisi Facebookille noin miljardi dollaria vuodessa.[244] Facebookin liikevoitto vuonna 2019 oli 24 miljardia dollaria ennen veroja. Investoinnin koko olisi alle 5 % sen liikevoitosta. Facebook oli myös maailman 14. tuottoisin yritys vuonna 2019 eikä tämä investointi todennäköisesti riittäisi edes pudottamaan sitä sijalle 15.[245]

Samalla Facebook on kuitenkin itse, muiden sosiaalisen median alustojen kanssa, disinformaatiokriisin keskustassa. Facebookin toistuvat kieltäytymiset puuttua asiaan tekevät siitä yhtä syyllisen tapahtumiin. Suojellessaan Kiinan, Venäjän, Iranin ja Myanmarin kaltaisia toimijoita, Facebook tulee osalliseksi näiden rikoksiin.

5.1. Toimenpide-ehdotukset ja Facebook

Disinformaation ongelmaa on mahdoton ratkaista ilman alustojen, tässä erityisessä tapauksessa Facebookin, yhteistyötä. Facebook on kieltäytynyt työskentelemästä yhdessä lainsäätäjien ja viranomaisten kanssa. Miten Facebookin suhteen tulisi siis toimia?

---

[240] https://www.wired.com/story/stop-saying-facebook-too-big-to-moderate/
[241] Ibid.
[242] https://www.reuters.com/article/us-facebook-languages-insight/facebooks-flood-of-languages-leave-it-struggling-to-monitor-content-idUSKCN1RZ0DW
[243] Barret. P. 2020. *Who Moderates the Social Media Giants? A Call to End Outsourcing*. Center for Business and Human Rights.
[244] https://www.wired.com/story/stop-saying-facebook-too-big-to-moderate/
[245] https://asian-links.com/gdp/most-profitable-companies

Koska alustat eivät itse ei ole valmiita ratkaisemaan ongelmaa, joiden luomisesta ne kantavat merkittävää vastuuta, mutta koska ongelma on samaan aikaan niin pakottava, ettei sen olemassaoloa voida enää ohittaa, lainsäätäjien on pakko puuttua alustojen toimintaan lainsäädännön kautta. Facebookia ja muita sosiaalisen median alustoja täytyy säädellä ja samalla ne täytyy velvoittaa vastuullisiksi disinformaation pysäyttämisessä. Samanaikaisesti niille täytyy asettaa todellisia sanktioita tilanteissa, joissa ne tahallisesti jättävät nämä toimet täyttämättä tai toimivat muuten lainvastaisesti. Sanktioiden täytyy myös olla riittäviä vaikuttamaan alustojen toimintaan.[246]

Tässä on myös toinen syy sille, miksi nykyinen malli ei ole toiminut alustojen kohdalla. Nykyisen säätelyn asettamat sanktiot ovat liian pieniä, jotta ne johtaisivat merkittäviin vaikutuksiin tai muutoksiin alustojen toiminnassa. Samalla niiden perustajat, jotka ovat tulleet miljardööreiksi alustojen kautta, välttävät rikosoikeudelliset seuraukset ja vastuun toimistaan.

Nämä ongelmat vaativat yhteiskunnan toimenpiteitä. Viimeinen osio esittelee kolme laajaa, normatiivista toimenpide-ehdotusta, jotka tarjoavat mahdollisuuden löytää ratkaisuja alustojen ja laskennallisen propagandan aiheuttamaan ongelmaan. Toimenpide-ehdotukset pohjautuvat sekä työn aikana esitettyihin ongelmiin, että ilmiöstä muodostuneihin havaintoihin. Ennen kaikkea, niiden olisi kuitenkin tarkoitus estää

[246] Yhdysvaltain FTC:n vuonna 2019 asettama sakko Facebookin yksityisyyspetoksesta, jossa se valehteli käyttäjilleen heidän datansa yksityisyydestä oli 5 miljardia dollaria. Se ei kuitenkaan aseta Facebookia rikosoikeudelliseen vastuuseen, tuo sanktioita sen toimitusjohtajalle tai johtoryhmälle, eikä ole riittävän suuri vaikuttaakseen sen käytökseen tulevaisuudessa. Yrityksen 70 miljardin dollarin kokonaisliikevaihdossa 5 miljardin dollarin sakko on reilusti alle kymmenesosa sen vuotuisesta liikevaihdosta, eikä edes neljäsosa sen liikevoitosta. Samaan aikaan sen petos on poikkeuksellisen törkeä ja Facebookille itselleen tuottoisa rikos. Facebook myös tiesi ongelmasta jo vuodesta 2015, jolloin se ilmoitti sijoittajille ”käyttäjien datan saattavan tulla väärin jaetuksi, julkaistuksi tai käytetyksi”. Voidaan siis sanoa Facebookin olleen selkeästi tietoinen asiasta ja samalla myös tehneen laskelmoidun päätöksen antaa asian jatkua jopa sakon uhalla. Koska sakko suhteessa sen kokonaistulokseen on niin pieni, on Facebookille silti kannattavampaa maksaa sakot ja jatkaa toimintaa samalla tavalla, kuin muuttaa toimintaansa lain mukaiseksi. Lähde:https://www.theguardian.com/technology/2019/jul/24/facebook-to-pay-5bn-fine-as-regulator-files-cambridge-analytica-complaint

lukujen 3.1 ja 3.2 kaltaisten tapausten toistuminen, tai ainakin antaa ensimmäiset mahdollisuudet taistella tämänkaltaisten tapausten toisintoa vastaan. Toimenpide-ehdotukset eivät ole kaikenkattavia tai yksityiskohtaisia, mutta ne edustavat suuntaa jonka kautta ongelma aikanaan voitaisiin ratkaista.

1. Lainsäädännön tulee puuttua sosiaalisen median alustojen toimintaan

Kuten aiemmassa osiossa käsiteltiin Facebookin esimerkin kautta, sosiaalisen median alustojen on lähes mahdotonta odottaa säätelevän itse itseään eikä sitä historian kautta voida pitää realistisena ratkaisuna ongelmaan. Alan toimijat, joista Facebook on esiintynyt ylivoimaisesti röyhkeimpänä, ovat toistuvasti rikkoneet niitä koskevia odotuksia, säännöksiä ja eettisiä ohjelinjoja. Niitä vastaan asetetut sanktiot ovat samanaikaisesti olleet liian pieniä vaikuttamaan niiden toimintaan eivätkä ole johtaneet aitoihin muutoksiin alustojen toiminnan osalta.

Sosiaalisen median jättiläiset tarvitsevat osakseen uudenlaista lainsäädäntöä ja säätelyä. Facebookia tulee sen omalta osalta pitää sekä syyllisenä että vastuullisena disinformaation ennennäkemättömästä ja suitsemattomasta leviämisestä. Se suojelee toimijoita tulemasta tunnistettavaksi. Samalla se reagoi toimintaan tai rikkomuksiin usein vuosia myöhässä. Facebook on myös toistuvasti asettanut omat talousetunsa yhteisön, käyttäjiensä ja yhteiskunnan etujen edelle syyllistyen röyhkeisiin laiminlyönteihin yksityisyyttä, terveyttä ja jopa fyysistä turvallisuutta kohtaan.

Lainsäädännön tulisi huomioida erityisesti sosiaalisen median alustojen yhteiskunnallinen rooli, niiden koko, tuottoisuus ja vastuullisuus ilmiössä. Lainsäädäntöä tulisi muokata tavalla, joka asettaa yhtiöille selkeät toimintaohjeet, valvonnan ja huomattavia sanktioita sekä johtotasolle yltävän rikosoikeudellisen vastuun rikkomuksista. Facebook itse tiesi Venäjän yrityksistä vaikuttaa Yhdysvaltain presidentinvaaleihin ainakin kesäkuusta 2016 alkaen, mutta tästä huolimatta se antoi toiminnan jatkua 18 kuukauden ajan häiritsemättä ennen operaatioon liitettyjen käyttäjätilien poistamista alustaltaan.[247]

[247] https://www.engadget.com/2017-09-25-facebook-russian-meddling-obama-zuckerberg.html

Lainsäädännön toteutumista tulisi valvoa esimerkiksi tätä tarkoitusta varten perustetun tai uudelleenmääritetyn kansallisen viranomaisen kautta, jolla olisi laajat toimivaltuudet sekä valvoa että pakottaa sosiaalisen median alustoja toimimaan lain puitteissa merkittävien rangaistusten ja sanktioiden kautta. Tämän viranomaisen tulisi olla riittävän toimivaltainen, että se voisi velvoittaa sosiaalisen median alustoja sekä valvomaan että torjumaan disinformaatiota omilla alustoillaan, mutta myös valvomaan itse sosiaalisen median alustojen toimintaa uudistetun lainsäädännön puitteissa.

Lainsäädäntöä olisi hyvä päivittää myös laskennallisen propagandan suhteen. Bottiverkostojen käyttäminen koordinoidun epäautenttisen käytöksen tai amplifikaation suhteen ei ole laissa kielletty toimintamuoto. Vaikka on vaikea sanoa, miten lainsäädännön tulisi puuttua tämänkaltaisiin toimintamuotoihin tai esimerkiksi laajamittaiseen pahantahtoiseen trollaamiseen, ne ovat samalla ilmiöinä niin laajalle levinneitä ja merkityksellisiä, että niiden käsitteleminen lainsäädännössä on tarpeellista. Samalla henkilökohtaisten hyökkäysten tekeminen ja laajamittainen häirintä tai vihapuhe sosiaalisessa mediassa on jotain, mihin yksityisten on vaikea saada apua sekä alustoilta itseltään tai viranomaisilta.

Lainsäädännön tulisi mahdollistaa näissä tapauksissa samanlaisia ratkaisuja joita se tarjoaa myös verkon ulkopuolella tapahtuvaan häirintään tai hyökkäyksiin. Samalla sen tulisi mahdollistaa, että viranomaisilla on sekä työkaluja että mahdollisuuksia tämänkaltaisissa tapauksissa yksilöiden suojelemiseksi sekä tekijöiden kiinnisaamiseksi ja pysäyttämiseksi. Useissa tapauksissa tekijät voivat piiloutua sosiaalisen median ja verkon tarjoaman anonymiteetin taustalle. Tämä tarkoittaa myös, että yksityisten on hyvin vaikea saada apua tilanteessa, jossa käyttäjä voi jatkuvasti luoda uusia tilejä, joiden kautta häirintää, uhkailua tai hyökkäyksiä ja vihapuhetta voidaan jatkaa anonyymisti. Sosiaalisen median alustojen olisi mahdollista työskennellä yhdessä viranomaisten kanssa tällaisen toiminnan pysäyttämiseksi ja tekijöiden saattamiseksi vastuuseen, mikäli lainsäädäntö velvoittaisi niitä tekemään niin, kuten sen tulisi.

2. Yhteiskuntien toimenpiteet disinformaation vastustamiseksi

Toistaiseksi laajamittaista sosiaalisen median kautta levitettävää disinformaatiota ja laskennallista propagandaa vastaan ei ole otettu merkittäviä askeleita. Pahantahtoiset

toimijat ovat voineet hyödyntää toimettomuuden tarjoamia mahdollisuuksia laukaistakseen laajempia disinformaatiokampanjoita ilman merkittävää vastusta.

Yhteiskuntien tulisi priorisoida kampanjoiden vastustaminen myös resilienssien rakentamisen kautta. Vastustuskykyä yhteiskunnissa olisi mahdollista rakentaa myös sosiaalisen median alustoihin puuttumisen ulkopuolella kouluttamalla kansalaisia. Parhaat mahdollisuudet tähän olisivat medialukutaidon parantaminen valeuutisten sekä mis- ja disinformaation tunnistamiseksi, että sen levittämisen pysäyttämiseksi. Sosiaalisen median alustat itse voisivat tukea tätä kamppailua parantamalla faktantarkistusta ja sisällön moderaatiota, varoittamalla käyttäjiä epäluotettavista uutislähteistä ja verkkosivuista sekä leimaamalla epäilyttävät uutiset ja tarjoamalla käyttäjille helpon keinon näiden ilmoittamiseksi. Samalla parempi medianlukutaito parantaisi kansalaisten omia kykyjä arvioida informaatiota ja epäluotettavia uutisia sekä hillitsisi näiden leviämistä lähtökohtaisesti.

Tätä työtä voitaisiin tukea esimerkiksi kansallisen viranomaisen perustamisen kautta, jonka tarkoitus olisi vastustaa disinformaatiota ja kouluttaa kansalaisia. Myös olemassa olevien toimijoiden resurssien lisääminen ja niiden vastuualueisiin dis- ja misinformaation torjunnan lisääminen olisivat mahdollisia vaihtoehtoja.

Kolmantena osana tulisi huomioida myös median roolin uudelleenarviointi sen vastuun suhteen disinformaation tuottajana. Vapaa media itsessään on äärimmäisen tärkeä ja keskeinen osa demokraattista yhteiskuntaa. Olisi kuitenkin tärkeä arvioida, missä määrin toistuvasti valheellisia uutisia ja mis- tai disinformaatiota levittävien julkaisujen tulisi sallia olla osa yhteiskuntaamme ja välttää vastuuta valheistaan. Julkaisut kuten suomalainen MV-lehti, yhdysvaltalainen Breitbart tai valtiolliset propagandaa levittävät julkaisut kuten Venäjän RT tai People’s Daily ovat selkeästi epäluotettavia kertojia ja ovat toistuvasti levittäneet joko harhaanjohtavia tai suoraan valheellisia uutisia ilman minkäänlaista totuusarvoa. Tämä pitäisi sekä tehdä selväksi, että siinä määrin kuin mahdollista, niitä pitäisi myös pitää vastuullisina julkaisemistaan uutisista.

3. Sosiaalisen median alustojen tulisi aloittaa yhteistyö tutkijoiden kanssa

Eräs keskeinen ongelma sosiaalisen median disinformaation ja laskennallisen propagandan tutkimuksen kanssa on viimeisten vuosien aikana ollut erityisesti Facebookin ja Googlen kieltäytyminen yhteistyöstä tutkijoiden kanssa. Alustojen läpinäkymättömyys on johtanut tilanteeseen jossa, hyvin harvoja poikkeuksia lukuun ottamatta, tutkijoiden on lähes mahdotonta tutkia suoraan laskennallista propagandaa tai disinformaation leviämistä Facebookissa.

Tämä aiheuttaa myös keskeisen haasteen esimerkiksi lainsäädännön ja koulutuksen kannalta. Koska ilmiöstä ja toimijoista olemassa oleva tutkimus on rajallista, on myös ilmiöön vastaaminen haastavampaa. Tämä johtaa myös korkeampaan läpinäkymättömyyteen, mikä samanaikaisesti suojaa toimijoita. Koska tutkijat ja esimerkiksi journalistit eivät voi yhtä lailla observoida käynnissä olevia disinformaatiokampanjoita, reaaliaikaisten vastausten muodostaminen niihin on haastavampaa. Tämä muodostaa tilanteen, jossa toimijat itse ovat aina askeleen edellä, sillä ne kykenevät toimimaan näkymättömistä eivätkä yleensä tule tietoisuuteen kuin vasta jälkikäteen, jos edes silloin.

Facebook on itse puolustanut lähestymistään kahdella tavalla. Ensiksi, se sanoo haluavansa suojella käyttäjiensä yksityisyyttä rajoittamalla käsiksi pääsyä tietoihin. Samalla se kieltäytyy jakamasta tunnistuskeinojaan pahantahtoisten toimijoiden tunnistamiseksi, etteivät toimijat itse voisi muuttaa toimintatapojaan vastauksena näihin. Toiseksi, Facebook sanoo datan jakamisen olevan liian ”raskasta” ja kieltäytyy osittain myös tästä syystä tekemästä niin.

Harkiten ensimmäistä syytä, sen käyttäjien yksityisyyttä, Facebookin argumentti ei ole täysin tyhjällä pohjalla. Tutkimuksen mahdollistaminen pitäisi tehdä tavalla, joka suojelisi käyttäjien yksityisyyttä ja anonymiteettiä eikä loukkaisi tai vahingoittaisi näiden oikeuksia. Toisaalta huomioiden, että Facebook on historiallisesti syyllistynyt lukemattomiin yksityisyysrikoksiin, jakaen käyttäjiensä datan Cambridge Analytican sekä monien muiden kaupallisten toimijoiden kanssa merkittävästi laajemmassa mittakaavassa, yksityisyys ei selvästikään ole Facebookin aito huoli asiassa. Tämä ei

tarkoita, etteikö käyttäjien yksityisyyttä pitäisi huomioida tutkimusta tehdessä, mutta se osoittaa, ettei tämä syy Facebookille itselleen selvästikään ole keskeinen motiivi.

Toisen syyn, siis prosessin ”raskauden” osalta, voidaan jälleen harkita Facebookin omia motiiveja. Datan jakaminen ja käsitteleminen tavalla, joka takaisi käyttäjien yksityisyyden ja turvallisuuden sekä erilaisten varmistus- ja yhteistyöprojektien aloittaminen epäilemättä maksaisi Facebookille hiukan. Mutta jos pahantahtoisten toimijoiden torjunta alustalta ei ole Facebookille tämän arvoista, se voi itsessään olla suurempi ongelma ja kertoa enemmän Facebookin omista motiiveista. Samalla datan jakamisen seurauksena tuleva tutkimus olisi epäilemättä moninkertaisesti arvokkaampaa kuin Facebookin mahdolliset investoinnit prosessiin ja sen tuoma tietoisuus, ja edut palaisivat moninkertaisina takaisin myös yhteiskunnalle. Samanaikaisesti Facebook voisi parantaa julkikuvaansa ja olla yhteiskunnallisesti vastuullisempi toimija, jos tämä kiinnostaisi sitä.

Vaikka tämä esimerkki on käsitellyt pelkästään Facebookia, sama voidaan ulottaa myös Googleen ja sen omistamiin palveluihin kuten Youtubeen sekä muihin sosiaalisen median alustoihin, jotka ovat yhtä lailla vastuussa ilmiöstä.

Pääsyn avaaminen tutkijoille tukisi myös kahta aiempaa toimenpide-ehdotusta lainsäädännöstä ja disinformaation torjumisesta. Kasvaneen tietoisuuden myötä paremmin valistuneiden lainsäädäntöesitysten suunnittelu olisi mahdollista ja kansalaiskoulutus ja disinformaation torjunta voitaisiin suunnata vastaamaan paremmin olemassa olevia tarpeita ja aktiivisia kampanjoita. Tätä kautta olisi mahdollista kehittää myös uusia keinoja, menetelmiä ja algoritmeja disinformaatiokampanjoiden reaaliaikaiseen torjumiseen sekä mahdollisesti tiettyjen laskennallisen propagandan menetelmien vastustamiseen.

Facebookin vihdoin ryhtyessä yhteistyöhön tutkijoiden kanssa olisi myös tärkeää, että tutkimukselle olisi saatavilla riittävästi resursseja. Esimerkiksi valtiot ja ylikansalliset toimijat voisivat kohdistaa tutkimusrahoitusta ilmiön laajemman ymmärryksen mahdollistamiseksi. Tällä hetkellä aiheesta tehtävä tutkimus on edelleen jossain määrin rajallista. Tutkimuksen rahallinen tukeminen olisi keskeinen osa ilmiön nopeammassa ymmärtämisessä sekä sitä kautta aktiivisessa torjunnassa ja vastustamisessa. Tämä on

kuitenkin sekä kansallinen että myös joidenkin ylikansallisten toimijoiden etu. Esimerkiksi dis- ja misinformaation torjunta pandemian yhteydessä on keskeinen osa taudin leviämisen pysäyttämistä. Tässä suhteessa valheellisen informaation pysäyttäminen ei ole yhden vaan kaikkien toimijoiden edun mukaista.

5.2. Loppusanat

Kuten luvun alussa todettiin, työn johtopäätökset olivat jossain määrin yllättäviä ja erosivat jossain määrin niistä painotuksista, joihin suurin asiasta tehtävästä tutkimuksesta keskittyy. Koen itse kuitenkin näiden johtopäätösten olevan eräs työn keskeisimmistä huomioista.

Vaikka itse toimijoiden ja laskennallisen propagandan keinojen ymmärtäminen on epäilyksettä tärkeää, tulisi myös alustojen roolia sekä vastuullisina osapuolina että itse ilmiön mahdollistajina korostaa. Samalla olisi tärkeää keskustella laajemmin myös siitä, kuinka suuri osa vastuusta niiden osalle kuuluu sekä mitkä ovat askelia, joita niiden voisi realistisesti olettaa ottavan. Tässä yhteydessä laajemmassa yhteiskunnallisessa keskustelussa tulisi harkita myös vahvemman säätelyn ja uuden lainsäädännön roolia. Vaikka työ itse asettaa toimenpide-ehdotukset aiheen suhteen, olisi keskustelun osalta tärkeää kuulla ja osallistaa myös lainsäätäjiä ja eri alojen asiantuntijoita. Samalla ilmiön vaikutukset ovat niin laajat, ettei keskustelun aloittamista tulisi lykätä pidempään.

Laskennallisen propagandan ja disinformaation seuraukset vaikuttavat meihin kaikkiin. Riippumatta omasta kyvystämme olla lähdekriittisiä ja valistuneita muut yhteiskuntamme jäsenet eivät aina välttämättä ole sitä. Samalla riippumatta siitä, miten hyvin huolehdimme omasta valistuneisuudestamme, emme myöskään ole riippumattomia kanssakansalaisistamme. Yhteiskunnassa, jossa jokaisen yksilön ääni on yhtä tärkeä, on myös jokainen disinformaatiolle altistunut kansalainen yhtä suuri menetys ja askel kohti vähemmän vapaata, heikommin valistunutta ja epäreilumpaa yhteiskuntaa.

Kysymys onkin siitä, kuinka paljon arvostamme totuutta ja kuinka haitallisiksi arvotamme valheet. Haluammeko antaa pahantahtoisen, mahdollisesti vieraan vallan toimijan aktiivisesti vaikuttaa siihen, millaisia päätöksiä yhteiskuntamme tekee? Välitämmekö siitä, että koronaviruspandemian, ennenkokemattoman yhteiskunnallisen kriisin kohdatessamme, jotkut toimijat näkevät haavoittuneisuudessamme tilaisuuden?

Olemmeko valmiita uhraamaan ihmishenkiä, unohtamaan rakastamiemme alustojen roolit menetyksissä, rikoksissa, kuolemissa jopa kansanmurhissa. Unohdammeko perusperiaatteen siitä, että vapautemme yhteiskunnassa nojaa vastavuoroiseen vastuuseen omasta toiminnastamme?

Nämä kysymykset ovat ongelman ytimessä. Mikäli välitämme totuudesta, teemme myös disinformaation pysäyttämisestä prioriteetin yhteiskunnassamme. Mikäli epäonnistumme tässä, se tarkoittaa, että lopuksi maksamme itse hinnan epäonnistumisestamme. Samanaikaisesti luovumme oikeudesta vaatia vastuuseen niitä osapuolia, jotka eivät vain johtaneet meitä tilanteeseen vaan tekivät itsestään miljardöörejä sen kautta.

Liitteet

1. Aineisto

Tärkein työssä käytetty aineisto on Oxfordin Yliopiston Internet Instituten *The Computational Propaganda Projectin* työt ja julkaisut viimeisten vuosien ajalta. Yksikön tuottama vuosittainen katsaus, ”Global Inventory of Organized Social Media Manipulation” vuodet -17 ja -19 ja sen katsaukset Covid-19 pandemian aikana leviävään valtiolähteiseen disinformaatioon ”Coronavirus Coverage by State-Backed English-Language News Sources” ja “Covid-19 News and Information from State-Backed Outlets Targeting French, German and Spanish-Speaking Social Media Users”, sekä Samuel Woolleyn ja Philip Howardin kirjoittama “Computational Propaganda: Political Parties, Politicians, and Political Manipulation” olivat hyvin keskeisiä lähteitä.

Philip Howardin ja kumppaneiden Yhdysvaltojen senaatin tutkinnan tueksi tehty raportti “The IRA, Social Media and Political Polarization in the United States, 2012-2018”, sekä *New Knowledgen* saman datan pohjalta tuottama “*The Tactics & Tropes of the Internet Research Agency*” ovat yhdessä senaatin oman tutkinnan raportin “Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election” osien I ja II kanssa keskeisiä erityisesti kolmannen luvun kannalta. Tätä tuki myös Robert Muellerin Yhdysvaltain oikeusministeriölle kirjoittaman “Report on The Investigation Into Russian Interference in the 2016 Presidential Election” osat I ja II.

EEAS:n East StratCom Task Forcen projekti ”EUvsDisinfo” ja sen julkaisut, muun muassa ”EEAS. 2020. *EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the Covid-19 Pandemic. (Update 23 April – 18 May)”*, sekä sen arkistoimat esimerkit valtiollisesti tuotetusta koronavirus-disinformaatiosta auttoivat kokonaiskuvan muodostamista ilmiöstä ja olivat keskeisessä osassa luvussa 3.

Muu osuus aineistosta koostuu eri sanomalehtien ja uutissivustojen, kuten The Guardianin, New York Timesin, The BBC:n, Reutersin, The Washington Postin, The Vergen, The Wiredin sekä uutissivustojen uutisoinnista ja artikkeleista ja lukuisista yksittäisistä tutkimusartikkeleista. Kunniamaininnan tutkimusartikkeleista ansaitsee erityisesti Christian Gimmen sekä kumppaneiden vuoden 2017 julkaisu ”Social Bots”

Human-Like by Means of Human Control?”, joka tarkastelee erilaisten bottien toimintaa, luomista ja käyttöä sosiaalisessa mediassa.