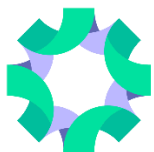


Sosiaalisen median toimijoiden rooli vakavissa kriiseissä ja poikkeusoloissa



Huoltovarmuusorganisaatio
Mediapooli



Laura Halminen, Harto Pönkä
Maaliskuu 2026
Tilaaja: Huoltovarmuusorganisaation Mediapooli



Johdanto: informaatioympäristö uhattuna	4
Suomalaisten sosiaalisen median käyttö.....	5
Mikroblogit ja viestipalvelu	5
Suomalaisten kokemuksia disinformaatiosta ja vihapuheesta sosiaalisessa mediassa.....	6
Digipalveluasetuksen velvoitteet suurille somepalveluille ja DSA-läpinäkyvyysraportit	6
VLOP-palvelujen läpinäkyvyysraportit	7
VLOP-palvelujen suomenkielisen sisällön moderointi	8
VLOP-palvelujen DSA:n mukaiset ilmoitukset ja poistopyynnöt Suomessa	9
Artikla 9:n mukaiset viranomaisten poistopyynnöt	9
Artikla 10:n mukaiset viranomaisten tietopyynnöt	9
Artikla 16:n mukaiset viranomaisten ilmoitukset	9
Artikla 16:n mukaiset luotettujen ilmoittajien ilmoitukset	10
Somepalveluihin liittyvien riskien tarkastelu	10
YouTube.....	11
Yhteenveto YouTubeen liittyvistä riskeistä	12
Facebook	12
Yhteenveto Facebookiin liittyvistä riskeistä	13
Instagram	14
Yhteenveto Instagramiin liittyvistä riskeistä	14
X	15
Yhteenveto X:ään liittyvistä riskeistä	16
TikTok	16
Yhteenveto TikTokiin liittyvistä riskeistä	17
Telegram	18
Yhteenveto Telegramiin liittyvistä riskeistä	19
Johtopäätökset	19
Liite: Ohjeita toimituksille poikkeustilanteisiin varautumisessa	21

Johdanto: informaatioympäristö uhattuna

Tämän raportin tavoitteena on tunnistaa ja välttää kriiseissä nähdyt karikot ja arvioida ennakoiden, miten suomalainen mediakenttä pystyy tukemaan yhteiskunnan vakautta nykyisessä sosiaalisen median ajassa oman tavoittavuutensa ja integriteettinsä säilyttäen. Lähtökohtina ovat sosiaalisen median käytön nykytila, suomalaisten valmiudet tunnistaa verkossa levitettyä disinformaatiota, sekä kansallisen ja eurooppalaisen lainsäädännön kuten digipalveluasetuksen (DSA) tarjoamien ilmoitusmahdollisuuksien arviointi.

Informaatioympäristössä kokonaisturvallisuudesta huolehditaan pitämällä huolta informaatioturvallisuudesta.¹ Huoltovarmuuskeskuksen mukaan informaatioturvallisuutta edistävät vahva demokratia, koulutus ja medialukutaito, avoin ja moniääninen kansalaiskeskustelu, sananvapaus, tiedon saatavuus ja riippumaton media.²

Moniääninen ja yleisön luottamusta nauttiva media on suomalaisen yhteiskunnan vahvuus. Luotettava media on osa yhteiskunnan informaatioresilienssiä ja kriisinkestävyyttä. Perusteeton median toimintaedellytysten nakertaminen voi olla uhka turvallisuudelle, sillä se luo otollista maaperää vihamieliselle vaikuttamiselle.

On keskeistä ymmärtää, millaiseen verkossa tapahtuvaan vihamieliseen informaatiovaikuttamiseen meidän tulee varautua. Informaatiovaikuttaminen on toimintaa, jolla pyritään vaikuttamaan yleiseen mielipiteeseen, ihmisen käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn. Vaikuttamisen keinoja ovat esimerkiksi väärrien tai harhaanjohtavien tietojen levittäminen ja painostaminen sekä sinänsä oikean tiedon tarkoitushakuinen käyttö.³

Vaikuttamisessa hyödynnetään pitkälle kehitettyä some- ja mediaseurantaa, sosiologista tutkimusta ja data-analyysiä, joka tunnistaa kohderyhmien käyttäytymismalleja sosiaalisessa mediassa sekä herkkyyksiä disinformaationarratiiveille.⁴ Trollitehtaat tuottavat valeuutissivustoja ja julkaisuja, joita levitetään sosiaalisen median palveluihin luotujen somekanavien, ryhmien ja tunnusten kautta. Generatiivisilla tekoälysovelluksilla sisällön tuottaminen on nopeaa, ja syvävääreännökset ovat tehokas keino luoda uskottavan tuntuista valheellista kuva-, ääni- ja videosisältöä.

Sosiaalisen median palvelujen moderointi ei kykene tai ole riittävän motivoitunut torjumaan taitavasti tuotettua valheellista ja harhaanjohtavaa sisältöä. Erityisen haavoittuvaisia ovat pienet kielialueet, joiden kielen vivahteita voidaan käyttää hyväksi niin, etteivät automaattiset moderointialgoritmit tunnista välttämättä edes julkaisun aihetta tai tiedon todenperäisyyttä. Väärää tietoa voidaan levittää myös tarkasti kohdennettuna sosiaalisen median mainosalustojen käytössä

¹ Valtioneuvosto, Yhteiskunnan turvallisuusstrategia: Valtioneuvoston periaatepäätös, 16.1.2025, <https://julkaisut.valtioneuvosto.fi/items/54938b49-dc3f-4a35-9a22-ad92f319e743>

² Huoltovarmuuskeskus, <https://www.huoltovarmuuskeskus.fi/mita-on-informaatioturvallisuus> (viitattu 11.1.2026)

³ Valtioneuvoston kanslia, Avoimesti, rohkeasti ja yhdessä - valtionhallinnon viestintäsuositus, 28.11.2016, <https://julkaisut.valtioneuvosto.fi/items/2914aac2-1cac-412b-9050-93ffe94e3796>

⁴ Pönkä Harto, 18.10.2024, <https://harto.wordpress.com/2024/10/18/sda-trollitehtaan-tietovuoto-osoitti-venajan-informaatiovaikuttamisen-olevan-huippuluokkaa/>

olevan profilointidatan avulla. Kuvaavaa on, että Meta arvioi vuoden 2024 mainosmyynnistään tulleen 10 % huijareilta ja muilta epäilyttäviltä tahoilta.⁵

Suomen mediakentän on välttämätöntä tuntea keinot, joilla disinformaatioon voidaan puuttua suurimmilla sosiaalisen median alustoilla. Tässä selvityksessä pyrimme löytämään tehokkaita toimintamalleja ja välineitä. Selvityksen on tilannut Huoltovarmuusorganisaatioon kuuluva Mediapooli.

Suomalaisten sosiaalisen median käyttö

Tavallisimmin sosiaalinen media yhdistetään käyttäjien sosiaalisista verkostoista rakentuviin yhteisöpalveluihin kuten Facebookiin, Instagramiin ja LinkedIniin. Niiden lisäksi somepalveluihin sisältyy mikroblogeja kuten X, Threads ja Bluesky, viestipalveluja kuten WhatsApp, Snapchat ja Telegram sekä videopalveluita kuten YouTube ja TikTok.

Suomalaisten sosiaalisen median palvelujen käytöstä on julkisesti saatavilla kolme vuosittain toistuvaa kyselyä: Tampereen yliopiston Uutismedia verkossa -kysely, joka on samalla osa Reuters instituutin Digital News Reportia, Uutismedian liiton kysely sekä DNA:n digitaalinen elämä -kysely. Suomessa suosituimmat sosiaalisen median palvelut olivat WhatsApp, YouTube, Facebook, Instagram, TikTok, Snapchat, Pinterest, Threads, X, LinkedIn ja Telegram.⁶

Mikroblogit ja viestipalvelu

Viime vuosien yksi merkittävimpiä muutoksia on ollut Twitterin (nykyisin X) päätyminen Elon Muskin omistukseen vuonna 2022. Muskin aikana X ei ole enää sitoutunut disinformaation vastaisiin käytäntönsäntöihin.⁷ Suomessa X:n vähentynyt käyttö on jossain määrin korvaantunut muiden samantyyppisten somepalvelujen käytön kasvulla, mutta vain LinkedIn ja Threads ovat pystyneet kilpailemaan X:n kanssa.

WhatsApp on sekä käytetyin viestisovellus että ylipäättään suosituin sosiaalisen median palvelu. Enemmistö opiskelu- ja työikäisistä käyttää WhatsAppia. Toiseksi suosituin pikaviestipalvelu on Facebookin Messenger. Kolmanneksi suosituin on Snapchat, ja sen jälkeen tulevat Telegram ja Signal.

Telegram on samaan aikaan pikaviestisovellus ja web-käyttöliittymän tarjoava somepalvelu, jonka kanavien tilaajamääriä ei ole mitenkään rajoitettu. Tämä on tehnyt Telegramista tehokkaan alustan myös disinformaation levittäjille. Telegramin käyttö on kasvanut Suomessa kahtena viime vuotena: 8 %:sta 13 %:iin.

⁵ Yle, 11.11.2025, <https://yle.fi/a/74-20193060>

⁶ DNA: Digitaalinen elämä 2025, <https://corporate.dna.fi/medialle/dnan-tutkimukset/digitaalinen-elama-2025>

⁷ Yle: Elon Muskin omistuksessa X-palvelusta on tullut pahin valeuutisten levittäjä – ”Me seuraamme mitä te teette”, varoittaa EU-komissaari, 26.9.2023, <https://yle.fi/a/74-20052091>

Suomalaisten kokemuksia disinformaatiosta ja vihapuheesta sosiaalisessa mediassa

Yhteiskunnallisessa keskustelussa sosiaalisen median varjopuolista puhuttaessa viitataan yleisesti nettikiusaamiseen, lasten hyväksikäyttöön, seksuaaliseen häirintään, vihapuheeseen, valeuutisiin ja disinformaatioon. Tässä selvityksessä keskitytään näistä teemoista disinformaatioon ja vihapuheeseen, jotka voivat liittyä valtiolliseen vaikuttamiseen kriiseissä ja poikkeusoloissa.

Kyselyjen mukaan disinformaatio kuten valeuutiset ja syväväärrennökset (deepfake) ovat suomalaisille yleinen ongelma verkossa. Sitä kohdataan erityisesti sosiaalisen median palveluissa, ja väärän tai harhaanjohtavan tiedon lähteinä korostuvat TikTok, X ja Facebook.⁸

Tilastokeskus on selvittänyt tieto- ja viestintätekniikan käytön kyselyissä epäilyttävien tietojen havaitsemista sosiaalisessa mediassa ja uutissivustoilla.⁹ Ihmisryhmiin kohdistuvia vihamielisiä ja halventavia viestejä oli nähnyt edellisen kolmen kuukauden aikana sosiaalisen median palveluissa tai uutissivustoilla 50 % vastaajista.

Digipalveluasetuksen velvoitteet suurille somepalveluille ja DSA-läpinäkyvyysraportit

EU:n digipalveluasetus (Digital Services Act, DSA) on tuonut suurille verkkoalustoille (very large online platforms, VLOP) uusia velvollisuuksia ja niiden toteuttamiseen liittyviä laajoja raportointi- ja läpinäkyvyysvelvoitteita vuodesta 2023 lähtien. Sosiaalisen median palveluista VLOP-palveluita olivat loppuvuodesta 2025 Facebook, Instagram, YouTube, TikTok, X, LinkedIn ja Snapchat.¹⁰ Euroopan komissio nimesi tammikuussa 2026 myös WhatsAppin VLOP-palveluksi sen kanavat ominaisuuden osalta.¹¹

Ennen digipalveluasetuksen voimaantuloa keskeiset sosiaalisen median palvelut ja muut suuret verkkoalustat sitoutuivat EU:n disinformaatiota koskeviin käytännönsäätöihin (Code of Practice on Disinformation, CoPD).¹² Disinformaatiota koskevat käytännönsäännöt laadittiin alun perin vuonna 2018 ja niitä vahvistettiin merkittävästi vuonna 2022.

⁸ Tampereen yliopisto: Uutismedia verkossa 2025. Reuters-instituutin Digital News Report - Suomen maaraaportti, <https://trepo.tuni.fi/handle/10024/229082>

⁹ Tilastokeskus: Väestön tieto- ja viestintätekniikan käyttö, <https://stat.fi/tilasto/sutivi>

¹⁰ Euroopan komissio: Supervision of the designated very large online platforms and search engines under DSA, 5.12.2025, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses>

¹¹ Euroopan komissio: Commission designates WhatsApp as Very Large Online Platform under the Digital Services Act, 26.1.2026, <https://digital-strategy.ec.europa.eu/en/news/commission-designates-WhatsApp-very-large-online-platform-under-digital-services-act>

¹² Transparency Centre: Discover the Code of Conduct on Disinformation, <https://disinfocode.eu/>

EDMO teki 2024–2025 monia EU-maita kattavan selvityksen disinformaatiota koskevien käytännėsääntöjen vaikutuksista sosiaalisen median alustojen toimintaan.¹³ Selvityksessä keskityttiin käytännėsääntöjen sitoumuksiin, jotka liittyvät käyttäjien, tutkimusyhteisön ja faktantarkastusyhteisön voimaannuttamiseen. Selvityksen mukaan somepalvelujen tekemät toimenpiteet ovat rajallisia, vaatimuksiin sitoutuminen epäjohdonmukaista eivätkä toimenpiteet disinformaation torjumiseksi vastaa somepalveluihin kohdistuvia odotuksia. Alle on tiivistetty kyselyn tulokset Metan, Microsoftin, Googlen ja TikTokin verkkopalvelujen osalta.

	Meta Facebook and Instagram	Microsoft Bing and LinkedIn	Google Search and YouTube	TikTok
User Empowerment	Mixed	Poor	Good	Fair
Fact-Checking Empowerment	Good	Poor	Good	Very poor
Research Empowerment	Excellent	Very poor	Good	Poor

Overview of VLOPSE Effectiveness Assessment on Selected CoPD Commitments

DSA:n laitonta vihapuhetta koskevia velvoitteita edelsi alun perin vuonna 2016 laaditut käytännėsäännöt disinformaatiopuheen torjumiseksi verkossa. Niillä on nykyisin 12 allekirjoittajaa, joista seitsemän on VLOP-palveluja: Facebook, Instagram, LinkedIn, Snapchat, TikTok, X ja YouTube. Uudistetut laitonta vihapuhetta koskevat käytännėsäännöt (The Code of conduct on countering illegal hate speech online) tulivat osaksi DSA:n kehystä tammikuussa 2025.¹⁴

VLOP-palvelujen läpinäkyvyysraportit

Yhtiöt aloittivat DSA:n edellyttämien läpinäkyvyysraporttien julkaisun syksyllä 2023. Tätä selvitystä varten on käyty läpi VLOP-palvelujen DSA-läpinäkyvyysraportit vuosilta 2023–2025.¹⁵ Raportit tarjoavat merkittävästi uutta tietoa somepalveluista paitsi digipalveluasetuksen velvoitteiden täyttämisestä kuten laittomaksi ilmoitetun sisällön käsittelystä ja muista moderointikäytännöistä, myös niinkin perustavanlaatuisesta seikasta kuin alustojen käyttäjämääristä eri EU-maissa.

Metan Facebookin ja Instagramin lukumäärät ovat pysyneet lähes muuttumattomina. Tätä voidaan pitää epäuskottavana, sillä kyselyjen tuloksista Facebookin käytön tiedetään laskeneen ja Instagramin nousseen Suomessa vuosina 2023–2025. Suurin suhteellinen muutos kirjautuneissa käyttäjissä nähdään X:ssä. Käyttäjien määrä kasvoi DSA-raporteissa peräti 67 %, vaikka kyselyjen perusteella todellinen käyttäjämäärä on ollut Suomessa laskussa.

¹³ European Digital Media Observatory: Implementing the EU Code of Practice on Disinformation: An Evaluation of VLOPSE Compliance and Effectiveness (Jan–Jun 2024), 24.6.2025, <https://edmo.eu/publications/implementing-the-eu-code-of-practice-on-disinformation-an-evaluation-of-vlopse-compliance-and-effectiveness-jan-jun-2024/>

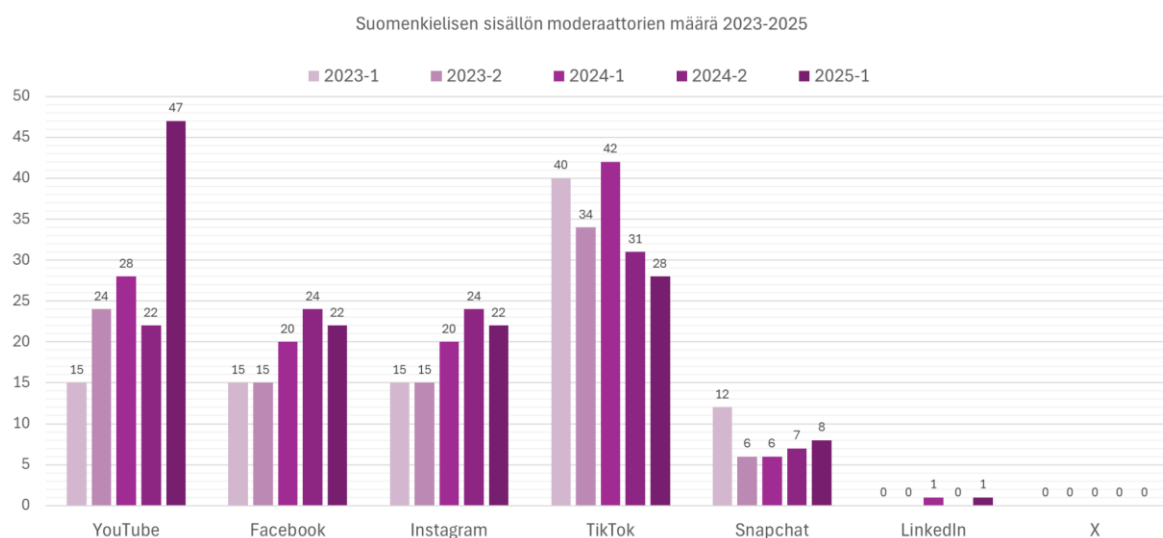
¹⁴ Euroopan komissio: Käytännėsäännöt verkossa esiintyvän laittoman vihapuheen torjumiseksi +, 20.1.2025, <https://digital-strategy.ec.europa.eu/fi/library/code-conduct-countering-illegal-hate-speech-online>

¹⁵ Euroopan komissio: Supervision of the designated very large online platforms and search engines under DSA, <https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses> (viitattu 13.1.2026)

VLOP-palvelujen suomenkielisen sisällön moderointi

Pienten kielialueiden sisältöjen moderoinnin voidaan olettaa olevan sosiaalisen median palveluille vaikeampaa kuin suurempien kielten. DSA-avoimuusraportit ovat tuoneet uudella tavalla esiin sen, kuinka paljon eri somepalvelut ovat resursoineet moderoijia suomenkielisen sisällön valvontaan. Tosin näihinkin lukuihin on syytä suhtautua varauksella, sillä kyse on yhtiöiden omista ilmoituksista.

Seuraavassa kuvaajassa on suomenkielisen sisällön moderaattoreiden lukumäärät eri sosiaalisen median palveluissa DSA-raporttien mukaan 2023–2025.



YouTuben moderoijien lukumäärän kasvu ei suoraan kerro suomenkielisen sisällön valvonnan resurssien lisäämisestä, vaan kyse voi myös siitä, että yksittäisten moderoijien vastuulla on aiempaa useampia kieliä. Metan Facebookin ja Instagramin moderoijat ovat yhteisiä molemmille palveluille, eikä suomenkielisen sisällön moderoijien lukumäärässä ei ole tapahtunut viimeisen kahden vuoden aikana merkittäviä muutoksia.

TikTokin DSA-raporteissa erotellaan kielelle “omistetut” (eng. dedicated) moderaattorit sekä kaikille kielille yhteiset moderaattorit. Suomenkielisen sisällön moderoijien lukumäärä laski merkittävästi 2024–2025 ja vastaava lasku on tapahtunut myös koko EU-alueella. TikTok on kertonut panostavansa sisältöjen automaattiseen moderointiin.¹⁶

X:n julkaisemien DSA-raporttien mukaan sillä ei ole kielikohtaisia moderointitiimejä. Sen sijaan se raportoi niiden moderaattoreiden määrän, jotka puhuvat ensi- tai toissijaisesti jotain EU-maiden kielistä. Raporttien mukaan X:llä ei ole yhtäkään suomenkielentaitoista moderaattoria, mitä voidaan pitää huomattavana riskinä sekä X:n omia sääntöjä rikkovan sisällön että laittoman sisällön leviämiseksi palvelussa.

¹⁶ TikTok: Digital Services Act Reporting, 2024–2025, <https://www.TikTok.com/transparency/en/dsa-transparency/>

VLOP-palvelujen DSA:n mukaiset ilmoitukset ja poistopyynnot Suomessa

Digipalveluasetus asettaa suurille sosiaalisen median palveluille velvollisuuksia, miten ilmoituksia laittomasta sisällöstä sekä viranomaisten poisto- ja tietopyyntöjä tulee käsitellä. Artiklat 9, 10 ja 16 määrittävät keskeiset toimintamekanismit viranomais määräyksille ja käyttäjien tekemille ilmoituksille. Artikla 15 puolestaan määrää, miten niistä pitää raportoida DSA:n mukaisissa avoimuusraporteissa.

Artikla 9:n mukaiset viranomaisten poistopyynnot

Tähän mennessä DSA-raporttien mukaan suomalaiset oikeus- ja hallintoviranomaiset ovat esittäneet artiklan 9 mukaisia sisältöjen poistomääräyksiä suurille sosiaalisen median palveluista Facebookille 1 kpl, Instagramille 6 kpl ja TikTokille 3 kpl.

Viranomaiset ovat siten käyttäneet varsin niukasti mahdollisuutta tehdä laittomien sisältöjen poistopyyntöjä. Viranomaisten edustajat ovat viitanneet esimerkiksi sosiaalisen median valvomiseen osoitettujen resurssien rajallisuuteen. Tämä voi aiheuttaa ongelman, mikäli alustat eivät tue riittävästi laittoman sisällön poistamista omatoimisesti.

Artikla 10:n mukaiset viranomaisten tietopyynnot

DSA:n artikla 10 mukaisia tietopyyntöjä suomalaisviranomaiset ovat lähettäneet Facebookille 1 kpl, TikTokille 438 kpl, Snapchatille 1130 kpl, LinkedInille 5 kpl ja X:lle 36 kpl.

Viranomaisten tekemien tietopyyntöjen määrissä huomio kiinnittyy TikTokiin ja Snapchatin selvästi muita sosiaalisen median palveluja suurempiin lukuihin. Snapchat ei kerro tietopyyntöjen tyypeistä tarkempaa tietoa. TikTokiin raporteista käy ilmi, että useimmin tietopyynnot ovat liittyneet kansalliseen turvallisuuteen ja terrorismiin (28 %), lasten hyväksikäyttöön (16 %) ja kunnianloukkaukseen (9 %). Vihapuheeseen liittyviä tietopyyntöjä on ollut vain 6 kpl (<1 %).

Myös X kertoo DSA-raporteissaan viranomaisten esittämien tietopyyntöjen laittomien sisältöjen kategoriat. Pyyntöjä on ollut verrattain vähän verrattuna TikTokiin. Useimmin tietopyynnot ovat liittyneet väkivaltaan (56 %), laittomaan tai haitalliseen puheeseen (19 %) ja alaikäisten suojeluun (14 %).

Artikla 16:n mukaiset viranomaisten ilmoitukset

Artikla 16:n mukaan sosiaalisen median palvelujen on tarjottava toimintoja, joiden avulla kuka tahansa yksityishenkilö tai yhteisö voi tehdä ilmoituksen sisällöistä, joita tämä pitää laittomana. Ilmoitustoimintojen on oltava helposti käytettävissä ja käyttäjäystävällisiä. Tavallisesti ilmoitustoiminto on toteutettu sosiaalisen median julkaisujen yhteydessä olevalla liputus- tai raportointitoiminnolla. Tämän lisäksi palvelut ovat tehneet erilaisia sähköisiä ilmoituskanavia mm. viranomaisille ja DSA:n artikla 22:n mukaisille luotetuille ilmoittajille.

X on tehnyt lainvalvontaviranomaisille oman ilmoituslomakkeen, jolla voi lähettää ilmoituksia hätätilanteista ja laittomaksi epäilystä sisällöstä.¹⁷ Kyse on matalan kynnyksen keinosta pyytää X:n

¹⁷ X: Legal request submissions, https://legalrequests.twitter.com/forms/landing_disclaimer

moderaattoreita tarkistamaan, rikkooko sisältö palvelun käyttöehtoja, jolloin moderaattorit voivat ryhtyä toimenpiteisiin kuten rajoittaa sisällön näkyvyyttä, lisätä siihen varoituksen tai poistaa sen. Tällaisia pyyntöjä on tehty runsaasti myös Suomen viranomaisten toimesta. Useimmin ilmoitukset ovat liittyneet väkivaltaan (31 %), laittomaan tai haitalliseen puheeseen (19 %), alaikäisten suojeluun (19 %) sekä huijauksiin ja petoksiin (12 %).

Artikla 16:n mukaiset luotettujen ilmoittajien ilmoitukset

DSA:n mukaan VLOP-palvelujen on käsiteltävä luotettujen ilmoittajien tekemät artikla 16:n mukaiset ilmoitukset priorisoituina ilman aiheetonta viivytystä.¹⁸ Tämä koskee yhtä lailla kaikkien EU-maiden kansallisen digitaalisten palvelujen koordinaattorien (DSC) hyväksymien luotettujen ilmoittajien tekemiä ilmoituksia. Suomessa DSC:n tehtävät ovat Liikenne- ja viestintävirasto Traficomilla.¹⁹

Luotettuja ilmoittajia on kartoituksen tekohetkellä yhteensä 64, joista suomalaisia on ainoastaan kolme: Tekijänoikeuden tiedotus- ja valvontakeskus ry TTVK, Pelastakaa Lapset ry ja Someturva-palvelua ylläpitävä Somis Enterprises Oy.

Pelastakaa lapset ry raportoi Nettivihje-palvelunsa DSA:n mukaisten ilmoitusten lukumääräksi 0 vuoden 2024 osalta.²⁰ Someturva teki vuonna 2024 kaikkiaan 14 ilmoitusta, joista puolessa tapauksista ilmoitus ei johtanut alustan toimenpiteisiin tai luotettu ilmoittaja ei saanut tietoa toimenpiteistä. Neljässä tapauksessa ilmoitettua sisältöä ei poistettu. Someturva kertoo tehneensä lisäksi noin 100 tavallista ilmoitusta sisällöistä, joita ei voitu ilmoittaa laittomana sisällönä.²¹

TTVK raportoi tehneensä yhteensä 56 DSA:n mukaista ilmoitusta vuonna 2024. Yksikään ilmoituksista ei kuitenkaan koske mitään edellä mainituista VLOP-palveluista, sillä TTVK keskittyy tekijänoikeusvalvonnan ilmoituksiin, jolle on erillinen DSA:n ulkopuolinen ilmoitusmenettely.²²

Somepalveluihin liittyvien riskien tarkastelu

Tyypilliset sosiaalisen median alustoihin liittyvät riskit liittyvät disinformaation levittämiseen, vihapuheeseen sekä DSA-raporteissa kuvattuihin palvelujen omia käyttöehtoja rikkoviin tai laittomiin sisältöihin. Yhteiskunnan informaatiointegriteetin ja luotettavan tiedonvälityksen kannalta huomio kiinnittyy informaatiovaikuttamiseen.

¹⁸ Euroopan komissio: Digitaalisia palveluja koskevan säädöksen mukaiset luotettavat ilmoittajat <https://digital-strategy.ec.europa.eu/fi/policies/trusted-flaggers-under-dsa>

¹⁹ Traficom: Luotetut ilmoittajat, 26.6.2024, <https://www.traficom.fi/fi/viestinta/datatalous-ja-digipalvelut/luotetut-ilmoittajat>

²⁰ Pelastakaa lapset ry: Nettivihje, 2025, <https://www.pelastakaalapset.fi/tyomme/mita-teemme/lasten-suojeleminen/seksuaalivakivallan-ennaltaehkaisy/>

²¹ Somis Enterprises Oy: Luotetun ilmoittajan vuosiraportti, 2025, <https://s3.eu-central-1.amazonaws.com/files.someturva.fi/trusted-flagger-report-2024.pdf>

²² Tekijänoikeuden tiedotus- ja valvontakeskus ry: Luotetun ilmoittajan vuosiraportti, 2025, https://ttvk.fi/assets/uploads/2025/02/luotetun-ilmoittajan-vuosiraportti-traficom-417_12.08.02_2025_ttvk.pdf

Tässä luvussa somepalveluihin liittyviä riskejä käydään läpi yhtiöiden ulkopuolisilla teettämien DSA-auditointien, niiden omien läpinäkyvyys- ja riskiarviointiraporttien, tehtyjen haastattelujen sekä muiden teemaan liittyvien lähteiden perusteella. Tähän tarkasteluun valittiin YouTube, Facebook, Instagram, X, TikTok ja Telegram.

YouTube

YouTube on Suomen käytetyin verkkovideopalvelu ja samalla merkittävä tiedonvälityksen ja mielipidevaikuttamisen alusta. Selvityksessä käytiin läpi Googlen julkaisemat DSA:n mukaiset järjestelmäriskien arviointiraportit YouTube:n osalta vuosilta 2024 ja 2025.²³ Oheinen kuva on NotebookLM-sovelluksen laatima tiivistelmä YouTube:n keskeisistä Suomeen kohdistuvan informaatiovaikuttamisen riskeistä.



Google tunnistaa riskiarvioinneissa YouTube:n suurimmiksi informaatiovaikuttamiseen liittyviksi uhiksi harhaanjohtavan tiedon levittämisen, koordinoituiden vaikutusoperaatiot sekä tekoälyn avulla tuotetun sisällön. Vaikka arviot koskevat koko EU:ta, monet niistä koskevat suoraan myös Suomea erityisesti vaalien ja kriisitilanteiden aikana.

YouTube:n suurin järjestelmätason riski on vihamielisten tahojen tuottama disinformaatio, jolla pyritään heikentämään luottamusta demokraattisiin prosesseihin ja kansallisiin instituutioihin. Generatiivinen tekoäly on muuttanut nopeasti informaatiovaikuttamisen mittakaavaa, sillä sen avulla voidaan tuottaa nopeasti suuria määriä realistisen tuntuisia kuvia ja videoita.

²³ Google: Report of Systemic Risk Assessments, 2024 ja 2025, <https://transparencyreport.google.com/?hl=fi>

Syväärennökset mahdollistavat myös julkisuuden henkilöiden ja poliitikkojen uskottavan imitoinnin, mikä vaikeuttaa käyttäjiä erottamaan aidon ja seipitetyn sisällön toisistaan.

Yhteenveto YouTubeen liittyvistä riskeistä

Osa-alue	Riski 1-3 (väri)	Tärkeimmät riskitekijät
Ilmoitustoiminnot käyttäjille ja luotetuille ilmoittajille	2	Pienen kielialueen moderoinnin vaikeus. Auditoinnissa havaitut puutteet luotettujen ilmoittajien ilmoitusten käsittelyssä.
Ilmoitustoiminnot medialle	2	Ei erillistä ilmoitustoimintoa medialle.
Ilmoitustoiminnot viranomaisille	2	Ei DSA:n 9 ja 10 artiklan mukaisia ilmoituksia Suomesta.
Käyttäjiin liittyvät riskit	2	Vihamieliset tahot voivat kiertää moderointia käyttämällä kieltä, jota automaattinen moderointi ei tunnista. Ei-kirjautuneiden käyttäjien suuri osuus raportoiduista vastaanottajista.
Alustan erityispiirteet ja poliittiset riskit	2	Google on vähentänyt yhteistyötä faktantarkistajien kanssa.

Facebook

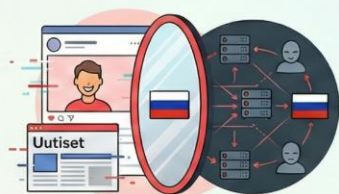
Facebook on edelleen maailman suurin yhteisöpalvelu. Metan alustoja käytti vuoden 2025 kolmannella neljänneksellä päivittäin jopa 3,54 miljardia ihmistä maailmanlaajuisesti.²⁴ Sen algoritmien toiminta vaikuttaa siten miljardien ihmisten tiedonsaantiin ja toimintaan. Suomessa on edelleen jopa 3,2 miljoonaa käyttäjää kuukaudessa. Alusta on osoittautunut hitaaksi, piittaamattomaksi tai jopa kyvyttömäksi poistamaan omien sääntöjensä vastaista mainontaa.

Selvityksessä käytiin läpi Metan Facebookia koskevat DSA:n mukaiset järjestelmäriskien arviointiraportit vuosilta 2024 ja 2025.²⁵ Oheinen kuva on NotebookLM-sovelluksen laatima tiivistelmä arviointiraporteista Facebookin keskeisistä Suomeen kohdistuvan informaatiovaikuttamisen riskeistä.

²⁴ Meta: Meta Earnings Presentation Q3 2025, https://s21.q4cdn.com/399680738/files/doc_financials/2025/q3/Earnings-Presentation-Q3-2025-Final.pdf

²⁵ Meta: Regulation (EU) 2022/2065 Digital Services Act (DSA) Systemic Risk Assessment and Mitigation Report for Facebook, 2024 ja 2025, <https://transparency.meta.com/reports/regulatory-transparency-reports/>

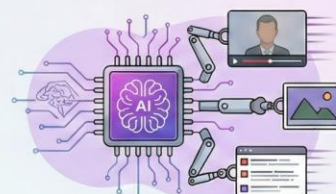
Informaatiouhat Suomessa: Metan alustojen keskeisimmät riskit



Venäjän "Doppelgänger"-operaatio
Tavoitteena on murentaa EU-maiden tukea Ukrainalle valeprofiilien ja valeuutissivustojen avulla.



Vaalivaikuttaminen ja keskustelun manipulointi
Poliittisia viestejä vahvistetaan keinotekoisesti, jotta ne näyttäisivät todellista suositumilta.



Tekoäly kiihdyttää harhauttamista
Mahdollistaa syväväärnönsten ja haitallisen sisällön massatuotannon ennennäkemättömällä nopeudella.



Koordinoitu epäaito toiminta
Verkostot harhaanjohtavat käyttäjiä tarkoituksellisesti henkilöisyydestään tai tavoitteistaan.



NotebookLM

Meta tunnistaa riskinarvioinneissa Facebookin suurimmiksi informaatiovaikuttamiseen liittyviksi uhiksi epäaidon toiminnan kuten ohjelmallisesti ohjatut tunnukset eli botit, valtiollisen vaikuttamisen sekä uusien teknologioiden, erityisesti tekoälyn, hyödyntämisen käyttäjien manipulaatioon pyrkivässä viestinnässä. Riskejä arvioidaan koko EU:n laajuisina ilmiöinä ja ne koskevat myös Suomea.

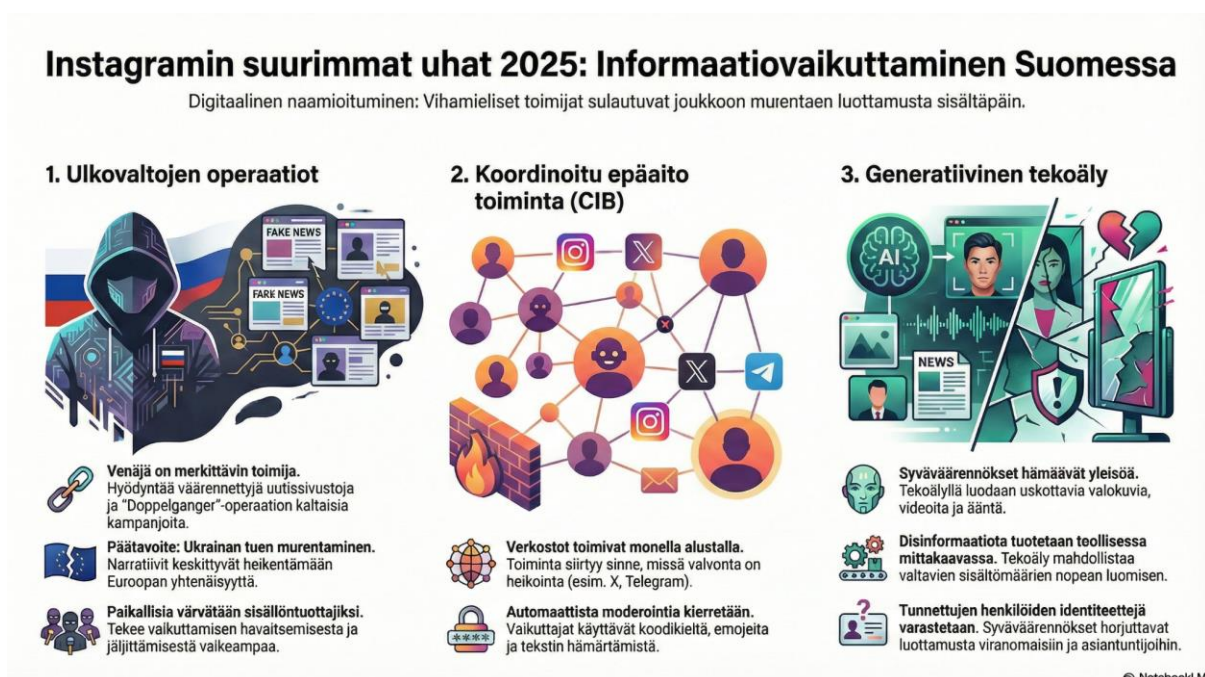
Yhteenveto Facebookiin liittyvistä riskeistä

Osa-alue	Riski 1-3	Tärkeimmät riskitekijät
Ilmoitustoiminnot käyttäjille ja luotetuille ilmoittajille	3	Ilmoitustoiminnot ja päätösten valitusmekanismit ovat komission virallisen tutkinnan alaisina.
Ilmoitustoiminnot medialle	2	Ei erillistä ilmoitustoimintoa medialle. Meta on vähentänyt yhteistyötä faktantarkistajien kanssa.
Ilmoitustoiminnot viranomaisille	2	DSA:n 9 ja 10 artiklan mukaisia ilmoituksia oli tehty vain yksi kumpaakin Suomesta.
Käyttäjiin liittyvät riskit	3	Huijaussisällöt ja mainokset ovat yleinen ongelma ja ne korostuvat pienellä kielialueella.
Alustan erityispiirteet ja poliittiset riskit	2	Meta on höllentänyt sääntöjään mm. vihapuheen osalta. Syötteen algoritmin toiminnassa on ollut aiemmin vakavia ongelmia ja

		viime vuosina algoritmissa on painotettu entistä enemmän “yhdistämättömiä julkaisuja” tahoilta, joita käyttäjä ei seuraa.
--	--	---

Instagram

Metan omistama kuvapalvelu Instagram ylitti vuonna 2025 globaalisti kolmen miljardin kuukausittaisen käyttäjän rajan. Selvityksessä käytiin läpi Metan Instagramia koskevat DSA:n mukaiset järjestelmäriskien arviointiraportit vuosilta 2024 ja 2025.²⁶ Oheinen kuva on NotebookLM-sovelluksen laatima tiivistelmä Instagramin keskeisistä Suomeen kohdistuvan informaatiovaikuttamisen riskeistä.



Instagramin rooli informaatiovaikuttamisen väylänä on kasvanut. Meta tunnistaa riskinarvioinneissa Instagramin suurimmiksi informaatiovaikuttamiseen liittyviksi uhiksi alustan käytön koordinoituihin vaikuttamisoperaatioihin, epäaitoon toimintaan sekä generatiivisen tekoälyn käyttöön.

Yhteenveto Instagramiin liittyvistä riskeistä

Osa-alue	Riski 1-3	Tärkeimmät riskitekijät
Ilmoitustoiminnot käyttäjille ja luotetuille ilmoittajille	3	Ilmoitustoiminnot ja päätösten valitusmekanismit ovat komission virallisen tutkimuksen alaisina.

²⁶ Meta: Regulation (EU) 2022/2065 Digital Services Act (DSA) Systemic Risk Assessment and Mitigation Report for Instagram, 2024 ja 2025, <https://transparency.meta.com/reports/regulatory-transparency-reports/>

Ilmoitustoiminnot medialle	2	Ei erillistä ilmoitustoimintoa medialle. Meta on vähentänyt yhteistyötä faktantarkistajien kanssa.
Ilmoitustoiminnot viranomaisille	2	DSA:n 10 artiklan mukaisia tietopyyntöjä ei oltu tehty Suomesta ainoatakaan.
Käyttäjiin liittyvät riskit	2	Bottitunnukset lisäävät riskiä disinformaatiolle.
Alustan erityispiirteet ja poliittiset riskit	2	Meta on höllentänyt sääntöjään mm. vihapuheen osalta. Instagramin syötteen algoritmin toiminnasta ei ole saatavissa läpinäkyvää tietoa.

X

X aloitti toimintansa Twitterinä vuonna 2006, kunnes Elon Musk osti palvelun vuonna 2022 ja nimesi sen seuraavana vuonna X:ksi. Muskin kaudella palvelun moderointia on heikennetty. Selvityksessä käytiin läpi X:n julkaisemat DSA:n mukaiset järjestelmäriskien arviointiraportit vuosilta 2024 ja 2025.²⁷ Oheinen kuva on NotebookLM-sovelluksen laatima tiivistelmä X:n keskeisistä Suomeen kohdistuvan informaatiovaikuttamisen riskeistä.

X-ALUSTAN JÄRJESTELMÄTASON RISKIT 2025: Informaatiovaikuttaminen EU-alueella

Huomio: Arviointi koskee yleisesti kaikkia EU-maita; Suomea ei mainita erikseen.



X tunnistaa riskinarvioinneissa suurimmiksi informaatiovaikuttamiseen liittyviksi uhiksi demokraattisiin prosesseihin kohdistuvan ulkomaisen vaikuttamisen, harhaanjohtavan tiedon

²⁷ X: DSA Systemic Risk Assessment Report, 2024 ja 2025, <https://transparency.x.com/en/reports/dsa-risk-assessment-report>

levittämisen sekä tekoälyteknologian lisääntyvän käytön. X ei riskinarvioinnissaan mainitse Suomea nimeltä, mutta sen tunnistamat uhkakuvat koskevat kaikkia EU-maita.

X:n toimia torjua tiedon manipulointia ohjaa sen omintakeinen ”freedom of speech, not reach” -periaate. Valheellisen sisällön laajan poistamisen sijaan ideana on rajoittaa sen näkyvyyttä. Lisäksi käyttäjälähtöiseen moderointiin perustuvat yhteisöhuomautukset tarjoavat harhaanjohtavalle sisällölle taustatietoa. X:n strategia eroaa huomattavasti useimmista muista keskeisistä sosiaalisen median palveluista, joiden moderointi keskittyy valheellisen sisällön poistamiseen.

Yhteenveto X:ään liittyvistä riskeistä

X:n riskitasoa nostaa Euroopan komission aloittamat viralliset tutkimukset, alustan viime vuosina tekemät moderointipolitiikan muutokset sekä sen laaja käyttö informaatiovaikuttamiseen.

Osa-alue	Riski 1-3	Tärkeimmät riskitekijät
Ilmoitustoiminnot käyttäjille ja luotetuille ilmoittajille	3	Ilmoitustoiminnot ovat komission virallisen tutkimuksen alaisina. Luotettujen ilmoittajien ilmoitusten käsittelyaika voi olla jopa pari kuukautta.
Ilmoitustoiminnot medialle	3	Ei erillistä ilmoitustoimintoa medialle. X on lopettanut yhteistyön faktantarkistajien kanssa.
Ilmoitustoiminnot viranomaisille	2	DSA:n 9 artiklan mukaisia poistopyyntöjä ei oltu tehty Suomesta ainoatakaan.
Käyttäjiin liittyvät riskit	3	Bottitunnukset lisäävät riskiä disinformaatiolle ja viime vuosina höllyennetyt säännöt laittomalle vihapuheelle.
Alustan erityispiirteet ja poliittiset riskit	3	X on ollut komission tutkimuksen alaisena liittyen lukuisiin DSA:n velvoitteisiin. X sai joulukuussa sakot DSA:n velvoitteiden rikkomisesta.

TikTok

Kiinalaislähtöisestä TikTokista on lyhyessä ajassa tullut yksi Suomen käytetyimmistä sosiaalisen median alustoista – erityisesti nuorten ja nuorten aikuisten keskuudessa. Samalla sen merkitys tiedonvälityksen ja mielipidevaikuttamisen kanavana on kasvanut.

Selvityksessä käytiin läpi TikTokin julkaisemat DSA:n mukaiset järjestelmäriskien arviointiraportit vuosilta 2024 ja 2025.²⁸ Oheinen kuva on NotebookLM-sovelluksen laatima tiivistelmä TikTokin keskeisistä Suomeen kohdistuvan informaatiovaikuttamisen riskeistä.

TikTok: Vaikuttamisen uhkakuvat Suomessa

TikTokin suurimmat turvallisuusriskit Suomessa liittyvät vaalien eheyden vaarantamiseen, tekoälyn hyödyntämiseen harhaanjohtamisessa sekä haasteisiin ymmärtää paikallista kieltä ja kulttuuria moderoinnissa. Vaikka alusta pyrkii torjumaan uhkia, merkittävä jäännösriski säilyy.

Keskeiset uhkakuvat: Vaalit ja tekoäly



Vaalihäirintä uhkaa demokratiaa
Luottamusta heikennetään levittämällä valheita ehdokkaista ja itse äänestysprosessista.



Tekoäly hämärtää totuuden ja fiktion rajaa
Realistiset syväväärennökset ovat tehokas työkalu informaatiovaikuttamisessa.



Uusi ilmiö: "Disinformaatio palveluna"
Vaikuttamisoperaatioita ja väärän tiedon levitystä voi nyt ostaa ulkopuolisilta toimijoilta.

Haavoittuvuudet: Paikallinen konteksti ja nuoret



Automaattinen moderointi ei ymmärrä Suomea
Hienovarainen suomenkielinen vaikuttaminen ja koodikieli jäävät usein tunnistamatta.



Nuoret ovat ensisijainen kohde
Heidän arvoihinsa ja maailmankuvaansa pyritään vaikuttamaan manipulatiivisella sisällöllä.



Turvallisuustyö on kuin suurkaupungin ylläpitoa
Uudet teknologiat, kuten tekoäly, vaativat jatkuvasti uudenlaista valvontaa ja sääntöjä.

NotebookLM

TikTok tunnistaa riskinarvioinneissa suurimmiksi informaatiovaikuttamiseen liittyviksi uhiksi vihamieliset pyrkimykset vaikuttaa vaaleihin, tekoälyn hyödyntämisen disinformaatiossa sekä paikallisen kielen ja kulttuurin ymmärryksen ongelmat automaattisessa moderoinnissa. Uutena ilmiönä TikTok on tunnistanut niin sanotun disinformaation palveluna, jossa informaatiovaikuttamisen operaatioita voidaan ostaa kaupallisilta toimijoilta.

Yhteenveto TikTokiin liittyvistä riskeistä

TikTokin riskitasoa nostaa Euroopan komission aloittamat viralliset tutkimukset sekä sen laaja käyttö informaatiovaikuttamiseen muun muassa Venäjän hyökkäyssodassa Ukrainassa sekä Romanian vaaleissa vuonna 2024.

Osa-alue	Riski 1-3 (väri)	Tärkeimmät riskitekijät
Ilmoitustoiminnot käyttäjille ja luotetuille ilmoittajille	3	Ilmoitusten käsittelyssä on ollut puutteita. TikTok on vähentänyt huomattavasti moderaattoreiden määrää EU:ssa 2024-2025.
Ilmoitustoiminnot medialle	2	Ei erillistä ilmoitustoimintoa medialle.
Ilmoitustoiminnot viranomaisille	2	Epäselvyydet ilmoitusmäärien raportoinnissa. Auditoinnissa

²⁸ TikTok: TikTok DSA Risk Assessment Report, 2024 ja 2025, <https://www.TikTok.com/transparency/en/dsa-transparency/>

		havaittu puutteita.
Käyttäjiin liittyvät riskit	3	TikTokia on käytetty laajasti informaatiovaikuttamiseen ja poliittiseen vaikuttamiseen vastoin alustan omia sääntöjä.
Alustan erityispiirteet ja poliittiset riskit	3	TikTok on ollut komission tutkinnan alaisena liittyen lukuisiin DSA:n velvoitteisiin ja sen käyttöön informaatiovaikuttamisessa Romanian vaaleissa 2024. TikTokin julkinen viestintä on osoittautunut epäluotettavaksi.

Telegram

Venäläislähtöinen viestipalvelu Telegram oli pitkään viranomaisten tavoittamattomissa, niin kutsuttu villi toimija. Telegram mahdollistaa jopa 200 000 käyttäjän kokoiset yhteisöt. Sen epäillään luistavan EU-lakien velvoittamista moderointivastuistaan. Sovelluksesta löytyy avoimesti propagandaa ja huumekauppaa sekä muuta rikollista sisältöä.²⁹

Telegram Suomessa: Uhkat ja Todellisuus

Uhkat ja Vaikuttamisen Keinot

Yli 2,6 miljoonaa roskapostitapausta EU:ssa
Roskapostitus on ylivoimaisesti suurin alustalla tunnistettu väärinkäytön muoto.

Petolliset arvonnat houkuttelevat yleisöjä
Kanavat keräävät seuraajia valheellisilla lupauksilla väylänä vaikuttamistoiminnalle.

Suomen viranomaisilta 66 tietopyyntöä
Pyynnöt osoittavat, että alustalla tapahtuu Suomen turvallisuuteen vaikuttavaa toimintaa.

Keskeinen Riskiä Pienentävä Tekijä

Ei sisältöä vahvistavia algoritmeja
Käyttäjät näkevät vain sisältöä kanavilta, joita he ovat itse päättäneet seurata.

Toimii kuin ilmoitustaulu, ei viraali syöte
Viestit tavoittavat vain oman yleisönsä eivätkä leviä algoritmien avulla laajemmalle.



²⁹ Reuters: Telegram's Durov says France asked to remove some Moldovan channels from app, 28.9.2025, <https://www.reuters.com/technology/telegrams-durov-says-france-asked-remove-some-moldovan-channels-app-2025-09-28/>

Telegram ei toistaiseksi ole DSA:n tarkoittama VLOP-palvelu, mutta se on julkaissut DSA:han liittyvän avoimuusraportin vuosien 2024–2025,³⁰ Oheinen kuva on NotebookLM-sovelluksen laatima tiivistelmä Telegramin keskeisistä Suomeen kohdistuvan informaatiovaikuttamisen riskeistä.

Yhtiön julkaisemien tietojen perusteella alustalla tunnistetaan useita väärinkäyttöön ja haitalliseen toimintaan liittyviä riskejä, jotka toimivat usein digitaalisen vaikuttamisen välineinä tai kanavina. Nämä riskit koskettavat myös Suomea ja Euroopan unionia.

Yhteenveto Telegramiin liittyvistä riskeistä

Koska Telegram ei ole selvityksen tekohetkellä VLOP-palvelu, sitä ei koske yhtä laajat velvollisuudet kuin muita edellä käsiteltyjä sosiaalisen median alustoja. Telegramin osalta ei myöskään ole saatavissa ulkopuolisen tahon tekemää riippumatonta auditointia.

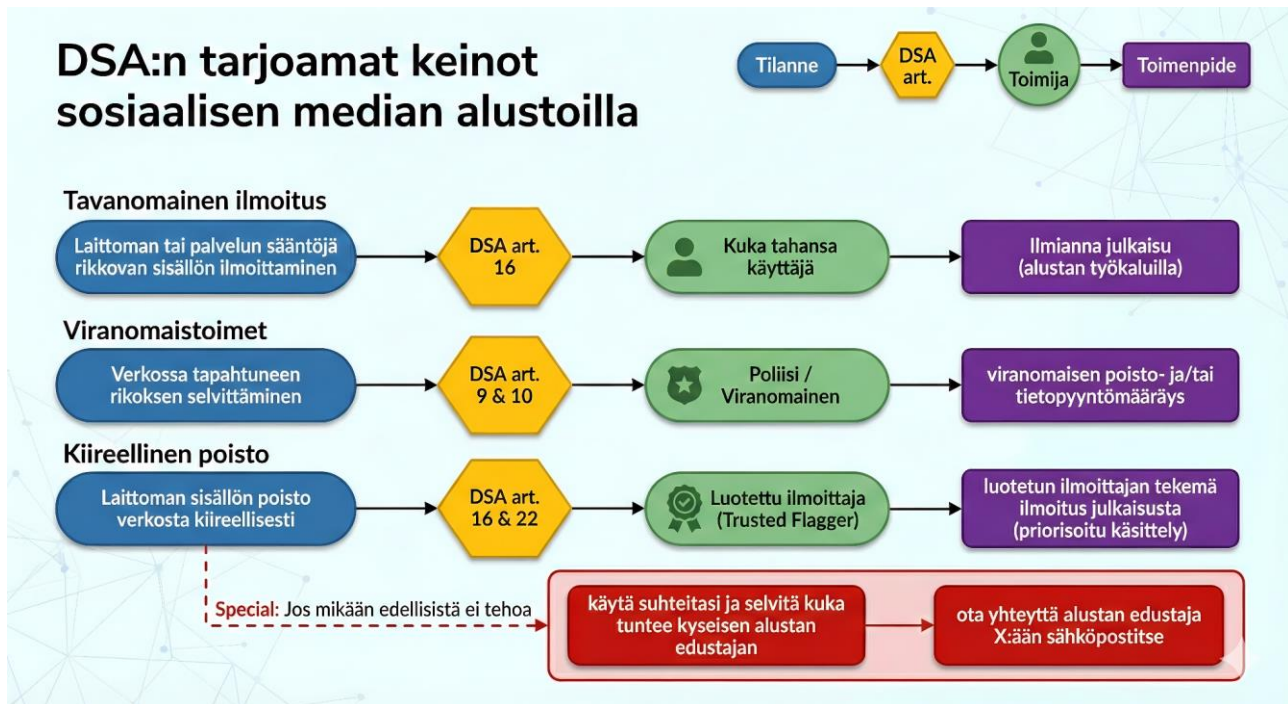
Osa-alue	Riski 1-3	Tärkeimmät riskitekijät
Ilmoitustoiminnot käyttäjille ja luotetuille ilmoittajille	2	Ei ulkopuolista auditointia.
Ilmoitustoiminnot medialle	2	Ei erillistä ilmoitustoimintoa medialle. Ei ulkopuolista auditointia.
Ilmoitustoiminnot viranomaisille	2	Ei ulkopuolista auditointia.
Käyttäjiin liittyvät riskit	3	Telegramia on käytetty laajasti informaatiovaikuttamiseen ja poliittiseen vaikuttamiseen.
Alustan erityispiirteet ja poliittiset riskit	3	Ei VLOP-palvelu, minkä takia ulkopuolinen DSA:n velvoitteiden valvonta on ollut vähäistä.

Johtopäätökset

Sosiaalisen median alustojen tehokkuus laittoman, häiritsevän ja uhkaavan toiminnan poistamiseksi tai torjumiseksi on hyvin vaihtelevaa. Myös haitallinen toiminta ja sisältö ovat erittäin monimuotoisia ja vaikuttamisen uhkaympäristö vähintäänkin kirjava. Yhdysvaltojen poliittinen tilanne ja Donald Trumpin hallinnon arvaamattomuus vaikuttaa alustojen tekemiin ratkaisuihin, mutta talvella 2026 ei vaikuttanut siltä että mikään alusta suunnittelisi vetäytyvänsä EU-alueelta. Alustat ovat kaupallisia toimijoita, ja Euroopan unioni käyttäjiineen on niille taloudellisesti vetovoimainen.

³⁰ DSA Transparency Report, <https://telegram.org/tos/eu-dsa/transparency-2025>

EU on kehittänyt suurimpiin digiyrityksiin ja -alustoihin kohdistuvaa sääntelyä. Vuonna 2024 täysimääräisesti voimaan tullut digipalveluasetus (Digital Service Act, DSA) sääntelee tiukimmin suuria verkkoalustoja (VLOP) ja hakukoneita, joilla on EU:ssa vähintään 45 miljoonaa kuukausittaista käyttäjää. DSA mahdollistaa alustojen tuntuvaan sakottamisen, mikäli ne eivät noudata asetuksen velvoitteita. Äärimmäisissä tapauksissa DSA mahdollistaa myös alustan toiminnan rajoittamisen EU:ssa kolmeksi kuukaudeksi kerrallaan.



Yksi keskeinen havainto on, että DSA:n tarjoamia ilmoitus- ja poistomekanismeja hyödynnetään Suomessa varsin rajallisesti. Viranomaisten artikloihin 9 ja 10 perustuvat poistopyynnot ja tietopyynnot ovat vähäisiä useimmilla alustoilla, ja luotettujen ilmoittajien asemaa ei ole vielä hyödynnetty täysimääräisesti. Käytännössä matalan kynnyksen artikla 16:n mukaiset ilmoitukset näyttäytyvät vähäisempien muotovaatimusten vuoksi toimivimpana keinona puuttua laittomaan tai haitalliseen sisältöön, mutta niiden vaikuttavuus vaihtelee suuresti alustojen välillä.

Samalla havaittiin, että DSA:n valvonta- ja sanktiomekanismeihin liittyy merkittävää hitautta, minkä vuoksi siitä ei ainakaan toistaiseksi uskota olevan kriisiaikojen työkaluksi. Pohdittavaksi jäi, tehostuisiko sosiaalisen median ongelmiin puuttuminen, mikäli Suomessa olisi luotettuja ilmoittajia jotka keskittyisivät informaatiovaikuttamiseen liittyvien julkaisujen ja tilien ilmoittamiseen.

Kriisitilanteessa yksittäinen uutistoimitus ei kykenisi vastaamaan laajamittaiseen informaatiovaikuttamiseen yksin. Tarvitaan tiiviimpää yhteistyötä median kesken, viranomaisten, kansalaisjärjestöjen ja faktantarkistajien kanssa sekä kitkattomia yhteyksiä somealustoihin.

Liite

Ohjeita toimituksille poikkeustilanteisiin varautumisessa

1. Tunne strategiset narratiivit

Omat strategiset narratiivit on tiedettävä ja tunnistettava ennakkoiden. On myös hyvä tuntee vastapuolen käyttämiä disinformaation narratiiveja, jotta omassa toiminnassa yleisöille voidaan tarjota siltä suojaavaa tietoa. Disinformaation torjumisessa tästä käytetään termiä prebunking, jonka voi tiivistää informaatiovaikuttamisen ennaltaehkäisyyn luotettavan tiedon ja kriittisen ajattelun avulla.

Esimerkiksi Venäjän Suomeen kohdistamia informaatiovaikuttamisen narratiiveja tunnetaan runsaasti ja niihin voi tutustua esimerkiksi EUvsDisinfo-tietopankin tapausten kautta.³¹ Strategiset narratiivit ovat merkityksellisiä jo kriisin alussa, sillä jos vinoa narratiivia ei korjata, se lukkiutuu alkutietojen varaan.³²

2. Varmista jatkuvuudenhallintasi ja priorisoi ydintehtävät

Pitkäkestoinen kriisi vie voimavaroja pitkään ja monimuotoinen kriisi vie voimavaroja myös yllättävistä paikoista. Taustahaastattelussa kävi ilmi, että erityisesti median kommenttikenttien sulkemista aikaisessa vaiheessa pidettiin järkevänä.³³ Tämän soveltamista myös sosiaalisen median tilien kommenttikenttiin on syytä harkita, sillä moderointi vie resursseja.

Sosiaalisen median kanavat ovat kuitenkin vuorovaikutuksen ja yleisön sitouttamisen kannalta erittäin merkityksellisiä, joten ratkaisut kommenttoinnin sulkemisesta on syytä harkita tarkasti ja rajata sulkeminen määräaikaiseksi tai julkaisukohtaiseksi.

3. Suojaa digitaalinen identiteettisi

Rekisteröi sosiaalisen median tilit valmiiksi käyttöön, jotta muut eivät voi ottaa niitä haltuun ja esiintyä valheellisesti organisaationasi. Sama koskee verkkotunnuksia (domain). Esimerkiksi Euroopan hybridiuhkien torjuntakeskus (HybridCOE) kohtasi alkumatkallaan runsaasti oikeushenkilöön kohdistuneita "identiteettivarkauksia" erilaisten sometilien, verkkotunnusten ja jopa yhdistyksen rekisteröimisen muodossa.³⁴

Pyri hankkimaan sosiaalisen median tileille alustan myöntämä merkintä tilin varmistamisesta aidoksi. Käytäntö toimii medioille Metan alustoilla luotettavammin kuin X:ssä. Omaa digitaalista identiteettiä muistuttavat tai hyväkseen käyttävät toisten perustamat tilit kannattaa viipymättä raportoida alustojen ylläpidolle. Varmista somekanavien ja -tunnusten hyvä salasanahygienia.

³¹ EUvsDisinfo, Database, <https://euvsdisinfo.eu/disinformation-cases/>

³² Haastateltava 2, 5.12.2025

³³ Haastateltava 1, 28.11.2025

³⁴ Laura Halminen: Hybridiuhkiin keskittyvä EU:n keskus Helsingissä sai riesakseen yhdistyksen, jonka taustalla on Johan Bäckman, 5.1.2017 <https://www.hs.fi/politiikka/art-2000005034628.html>

Käytä aina myös kaksivaiheista tunnistautumista ja käy säännöllisin väliajoin läpi keillä kaikilla on käyttöoikeus tileille.

4. Kouluta ja varaa henkilökunta

Kriisejä on monenlaisia nopeista ja akuuteista onnettomuuksista pitkäkestoiseen hybrdivaikuttamiseen ja täysimittaiseen sotatilaan. Resilienssiä eli psyykkistä palautumiskykyä voi tukea varautumisella ja harjoittelulla sekä kattavalla jälkihoidolla. Nopeiden kriisien jälkeen levon ja keskusteluavun mahdollistaminen on tärkeää. Defusing- ja debriefing-käytänteistä saa yleensä hyvin tietoja työterveyshuollon palveluina. Pitkäkestoisessa hybrdivaikuttamisessa on varauduttava siihen, että yrityksen henkilöstö muuttuu vaikuttamisen kohteiksi. Oikeusvaltion rakenteita voidaan pyrkiä käyttämään demokratian ja osallistumisen vastaisesti esimerkiksi slapp-kanteilla (*strategic lawsuit against public participation*).

Henkilökuntaan voi kohdistua myös pehmeämpää vaikuttamista, kuten lahjontaa, tiedustelua ja vaikuttamista seksi- ja rakkaussuhteiden muodossa (ns. "hunaja-ansat") sekä aitoja tietovuotoja. Journalistiset ihanteet ja median ydintehtävä vallan vahtikoirana voivat muodostaa tietovuototilanteessa eettisiä ristiriitoja, ja lähteiden motiivien suhteen on oltava erittäin tarkkana. Ukrainassa toimitusten työskentelyä on häiritty laajoilla pommiuhkausten aalloilla, kanavien sieppaamisella ja infrastruktuurin tuhoamisella, mutta toimittajia on myös siepattu ja kadonnut. Joidenkin surmaamiseksi on tilattu palkkamurha.³⁵

Osalla henkilökunnasta voi olla reservissä sodan ajan sijoitus, joka saattaa poiketa tavanomaisesta ammatista ja työnkuvasta paljonkin. Sodan ajan sijoitus voi erityistapauksissa olla myös ihmisellä, joka ei ole suorittanut asepalvelusta. Työnantaja ei sijoitusta saa kysyä, mutta erityisen ammatin harjoittaja voidaan jättää kutsumatta palvelukseen. Näin työnantaja, jolla on kriisissä keskeisiä tehtäviä kuten yleisen tiedonsaannin varmistaminen, voi pyrkiä varmistamaan, että organisaatiolla on riittävästi tehtävänsä kannalta olennaisia työntekijöitä. Puolustusvoimat käyttää tällaisesta viisi vuotta kerrallaan voimassa olevasta henkilövarauksesta termiä VAP, josta menettelylle on syntynyt puhekielinen nimi "vappaaminen". Henkilövaraus tehdään puolustusvoimien sivuilta löytyvällä lomakkeella varaajan kotipaikan aluetoimistoon, ja sen voi tehdä vain huoltovarmuuskriittinen yritys.³⁶

5. Rakenna vaikuttava yleisösuhte

Sosiaalinen media ei ole sosiaalinen, jos se ei ole vuorovaikutteinen. Osallista yleisöä, kysy, reagoi, ole läsnä. Vuorovaikutteisuus sitouttaa ja parantaa luottamusta. Kriisitilanteessa yleisösuhteesta on hyötyä: yleisö muistaa ja ymmärtää, missä se on tavoittanut median ja sen edustajat aikaisemmin. Näin he tietävät, mihin voivat tarjota itse saamaansa informaatiota, kuten kuvia ja uutisvinkkejä.

³⁵ BBC News: Arkady Babchenko: Ukraine faked murder of journalist, 30.5.2018, <https://www.bbc.com/news/world-europe-44307611>

³⁶ Puolustusvoimat: henkilövaraus, <https://puolustusvoimat.fi/henkilovaraushakemus>

6. Etsi kumppaneita ja verkostoidu

Toisilta saa oppia ja ajatuksia hyvistä käytänteistä ja tarvittaessa myös tukea voi pyytää. Tuttua ihmistä ja organisaatiota on yllättävän tilanteen tullen helpompi lähestyä kuin tuntematonta. Henkilökohtaiset suhteet toimivat myös muihin nähden luottamusta vahvistavana tekijänä. Yhteistyömalleja on syytä harkita myös journalistisessa työssä siltä varalta, että oman organisaation työmahdollisuudet yllättäen rajoittuisivat tai estyisivät esimerkiksi sähkökatkon tai kyberhyökkäyksen vuoksi.

Verkostoituminen myös sosiaalisen median jättien kanssa on osoittautunut hyödylliseksi. Taustahaastateltavat kertoivat, että henkilökohtaiset suhteet ovat olleet jopa ainoa keino saada ongelma ratkaistuksi. Jos itselläsi ei ole suhteita sosiaalisen median työntekijöihin, etsi verkostoistasi joku jolla on.

7. Osallista kansalaiset ja kolmas sektori

Suomessa on vireä ja monimuotoinen kolmas sektori. Esimerkiksi koronapandemian aikana Valtioneuvoston kanslia käytti sosiaalisen median vaikuttajia jakamaan oikeaa tietoa aihetunnisteella (hashtag) #faktaakoronasta.³⁷ Tämä ei tarkoita journalistisen päätäntävällän luovuttamista toimitusten ulkopuolelle, vaan monenlaisia jo tuttujakin yhteistyön malleja ja niiden tavoitteellista tehostamista: esimerkiksi joukkoistamista, näkyvyysyhteistyötä tai muita erilaisia projektimuotoisia yhteistyöhankkeita kuten vaikkapa juttusarjoja.

Konflikteja ja kriisejä määrittää epävarmuus ja vaikeus ennakoida tulevaa. Tällaisissa tilanteissa ihmisillä on tarve toimia asian puolesta ja osoittaa tällä psykologista minäpystyvyyttä. Osallistaminen sitouttaa ihmisiä ja luo merkityksellisyyden kokemusta, mutta mahdollistaa myös laajemman määrän ideoita ja voi sitä kautta parantaa lopputulosta. Tilannetta verrattiin yritysmaailmaan ja startup-sektoriin, jonka resursseja on jo opittu hyödyntämään tehokkaammin.³⁸ Tiedotusvälineillä ja toimituksilla on valtionhallintoa laajempi itsemääräämisoikeus ja toimintavapaus, joten ketteryys kansalaisyhteiskunnan kanssa on nykyäänkin monesti alihyödynnetty resurssi.

8. Harjoittele

Selvityksessä ilmi käyneiden taustatietojen perusteella suomalaisissa toimituksissa on harjoiteltu kriisitilanteita suhteellisen vähän. Poikkeuksen muodostaa Yleisradio, jolla on lakisääteinen tehtävä varmistaa tiedonvälitys myös poikkeusoloissa.

Pohdi, miten kriisi näyttäytyisi juuri sinun organisaatiossasi. Onko ihmisten toimenkuvia koulutettu ristiin siltä varalta, että työntekijöitä "putoaa pois"? Muistele koronapandemiaa: oliko organisaatiosi ydintoimintoja testattu siltä varalta, että niitä oli pakko ryhtyä käyttämään etäyhteyksillä? Varautuminen on avain onnistumiseen. Organisaatio ei ryhdy toimimaan toisin sillä, että pilliin vihelletään, vaan sillä, että toimintamallit on luotu ja sisäistetty. Kaikki mitä teemme ja kannamme

³⁷ Laaksonen, Salla-Maria ym: Koronakriisin julkinen dynamiikka -hanke, Koronakriisin jännitteinen julkisuus - loppujulkaisu, https://blogs.helsinki.fi/uncocoproject/files/2022/11/report_UnCoCo-KJD-lores.pdf

³⁸ Haastateltava 1, 28.11.2025, haastateltava 3 5.12.2025 & haastateltava 4, 29.12.2025



mukanamme, siirtyy myös kriisiaikaan. Mitään uutta sääntökirjaa kriisiaikaan ei saa mukaan, vaan se rakennetaan etukäteen rauhan ajassa.³⁹

Huoltovarmuuskeskuksen Digipooli järjestää joka toinen vuosi tietoyhteiskunnan viranomaisille ja huoltovarmuuskriittisille yrityksille suuren Tieto-valmiusharjoituksen. Muita harjoitusmahdollisuuksia voi tutkia esimerkiksi Naisten valmiusliiton ja Maanpuolustuskoulutusyhdistyksen (MPK) verkkosivuilta.

³⁹ Haastateltava 3, 28.11.2025