

Bottifarmien vaikutukset ja torjunta Euroopassa tekoälyn aikakaudella

TURUN YLIOPISTO
Tietotekniikan laitos
TkK-tutkielma
Tietotekniikka
Toukokuu 2026
Felix Arjasmaa

TURUN YLIOPISTO

Tietotekniikan laitos

FELIX ARJASMAA: Bottifarmien vaikutukset ja torjunta Euroopassa tekoälyn aikakaudella

TkK-tutkielma, 26 s.

Tietotekniikka

Toukokuu 2026

Viime vuosina ulkopuoliset tahot ovat lisänneet bottien käyttöä sosiaalisissa medioissa disinformaation levittämiseen. Tämän toiminnan tavoitteena on ollut vaikuttaa Euroopan maiden yhteiskuntiin ja eurooppalaisten maailmankuviin. Tässä tutkielmassa tarkastellaan bottifarmeja, eli useista yhteistyötä tekevistä boteista muodostuvia verkostoja. Tutkielmassa analysoidaan empiirisesti eri raportteja, jotka osoittavat bottifarmien vaikutuksia vaaleihin, yhteiskuntiin ja niiden polarisaatioon. Lisäksi käsitellään erilaisia lainsäädäntöjä, strategioita ja yhteistyösuunnitelmia, joita Euroopan unionin ja yksittäiset eurooppalaiset valtiot ovat toteuttaneet bottifarmien torjumiseksi. Lopuksi arvioidaan, kuinka tekoäly ja sen kehitys tulee vaikuttamaan bottifarmeihin ja niiden tunnistamiseen sosiaalisissa medioissa. Tutkielman perusteella näillä bottifarmeilla on laajat yhteiskunnalliset haitat, jotka tulevat todennäköisesti kasvamaan tulevaisuudessa. Samalla myös niiden vastainen toiminta on myös lisääntymässä, jonka vuoksi aihe tulee olemaan yhä tärkeämpi lähitulevaisuudessa.

Asiasanat: sosiaalinen media, tekoäly, hybridisota, vaikuttaminen, disinformaatio, eurooppa, euroopan unioni

Sisällys

1	Johdanto	1
2	Bottifarmit	4
2.1	Bottifarmit yleisesti	4
2.2	Käyttötarkoitukset ja menetelmät	6
3	Vaikutukset ja haitat	8
3.1	Poliittinen manipulointi	8
3.2	Sosiaaliset haasteet	10
3.3	Taloudellinen sabotointi	11
4	Eurooppalaisen kyberturvallisuussektorin kehitys ja yhteistyö	13
4.1	Sääntely ja lainsäädäntö	13
4.2	Turvastrategiat ja suojautuminen	15
4.3	Yhteistyö ja tiedonvaihto	16
5	Tekoälyn luomat hyödyt ja haitat	18
5.1	Skaalautuvuus ja personointi	18
5.2	Järjestelmät bottien tunnistamiseksi	19
5.3	Bias ja disinformaatio generatiivisella tekoälyllä	20
6	Pohdinta	22

7 Yhteenveto	24
Lähteluettelo	27

1 Johdanto

Vuonna 2024 noin 64,8 prosenttia Euroopan unionin väestöstä oli käyttänyt sosiaalista mediaa viimeisen kolmen kuukauden aikana (Euroopan unioni, 2024a). Sivustot ja sovellukset, kuten Facebook, X ja TikTok, ovat monelle Euroopan kansalaiselle keskeisiä tiedonlähteitä, joissa voi kuulla samankaltaisten, mutta kaukaisten ihmisten mielipiteitä ja ajatuksia eri aiheista. Nämä vaikuttavat käyttäjien sosiaalisiin, taloudellisiin sekä poliittisiin valintoihin arkielämässä. Palveluiden korkea käyttö ja niiden mahdollistama anonyymisyys antavat ulkopuolisille toimija myös mahdollisuuksia vaikuttaa eurooppalaisten päätöksiin yleisesti heidän huomaamatta. Käyttäjille voidaan liioitella tarkemmin katsottuna pieniä ongelmien vakavuudesta, vaelhdella esimerkiksi taloudellisesta tilanteesta tai luoda tarkoituksellisesti harhaanjohtavaa sisältöä tahojen vastaisista poliitikoista. Tämän kaiken voidaan tehdä automaattisesti ja helposti käyttämällä botteja, tarkemmin lukuisista boteista muodostuvaa koordinoitua verkostoa, eli ”bottifarmia”. Sosiaalisten medioiden sisältämissä keskusteluissa noin 20 prosenttia viesteistä on jo samanlaisten bottien tai bottifarmin tuottamia (Ng & Carley, 2025). Maailmanlaajuinen geopoliittinen tilanne on viime vuosina kiristynyt vakavasti. Euroopan komissio sanoo juuri tällaisen aggressiivisen informaatiovaikuttaminen ja sen torjumisen tulevan olemaan kärkiasemassa kansainvälisessä vaikutuksessa (Euroopan unioni, 2025a).

Bottifarmin tuoma uhka perustuu niiden jatkuvasti kasvavan määrän lisäksi niiden koordinoituun toimintaan tiedonjaossa. Tämä luo epätodellisen kuvan varsi-

naisesta kansallismielipiteestä eri aiheista, joista sillä hetkellä sosiaalisissa medioissa keskustellaan. Ihmiskäyttäjiin verrattuna botit voivat tuottaa ja levittää sisältöä näillä sivustoilla moninkertaisella nopeudella, jolloin suurempi osa sivujen käyttäjistä altistuu tälle väärälle tiedolle. (Stella ym., 2018) Bottiverkostojen uhka on kasvanut viimeaikaisten teknologisten kehityksien kautta, ja näistä erityisesti generatiivinen tekoäly (engl. Generative AI, GenAI) sekä kielimallit (engl. Large Language Models, LLM), jotka parantavat ja hienosäätävät bottien manipulointia vielä entistä paremmin (Lopez-Joya ym., 2025). Tämä kehitys on madaltanut kynnystä bottien hyödyntämiseen, jolloin bottifarmit muuttuivat suurten yhteisöjen ja valtioiden ylläpitämistä hankkeista palveluksi, joita voidaan käyttää pienimmilläkin resursseilla maailmanlaajuiseen vaikuttamiseen.

Tämän tutkielman aiheena on selvittää, millä tavalla bottifarmeja käytetään vaikutukseen sosiaalisissa medioissa, tutkia niiden vaikutuksia eurooppalaiseen elämään ja tarkastella keinoja, joilla eurooppalaiset valtiot ovat varautuneet torjumaan bottifarmien luomia ongelmia. Lopuksi tutkitaan generatiivisen tekoälyn vaikutuksia tähän kamppailuun. Esitellään eri tapoja, miten tekoäly on vaikuttanut ja tulee vaikuttamaan sekä miten se tulee muuttamaan pelikenttää sen vaikutusten ja puolustuksen suhteen. Tutkimuskysymykset muodostuivat seuraavalla tavalla:

TK1: Millaisia haittoja bottifarmit aiheuttavat Euroopassa?

TK2: Miten Euroopan kyberturvallisuussektori on kehittynyt bottifarmien torjuntaan?

TK3: Miten tekoäly on vaikuttanut bottifarmien toimintaan, ja miten sen rooli kehittyy tulevaisuudessa?

Tutkielma on toteutettu kirjallisuuskatsauksena. Tiedonhaku toteutettiin monessa eri palvelussa: Web Of Science, IEEE, Google Scholar, PubMed, ResearchGate ja ACM Digital Library. Aiheen tuoreuden ja kokoaikaisen kehittymisen vuoksi botti-

farmeista on niukasti tieteellisiä artikkeleita saatavilla, minkä vuoksi aiheen ympäriltä jouduttiin hakemaan tietoa eri hakusanoilla, kuten:

Taulukko 1.1: Hakusanat ja -aiheet

Pääaihe	Alueen rajaavat aiheet	Aiheeseen liittyvät muut hakusanat
Social media Bot	Europe Generative AI LLM	Disinformation Media Politics Propaganda Manipulation Fake news Social bot Algorithm Hybrid Warfare

Aiheen vuoksi varsinkin tutkimuskysymykseen 2 tarvittiin tieteellisten tietokantojen ulkopuolista tietoa, jolloin tietoa haettiin EU:n ylläpitämiltä palvelulta saadakseen eri aiheeseen liittyviä ja tukevia tutkimuksia, tilastoja sekä sopimuksia.

Luvussa 2 selitetään bottifarmeista sekä niiden käyttötarkoituksia ja -menetelmistä, kun taas luvussa 3 syvennyttään näiden verkostojen luomiin haittoihin ja vaikutuksiin monella eri tavalla. Eurooppalaista puolustuskykyä näitä uhkia vastaan tutkitaan luvussa 4, ja tekoälyn tuomia hyötyjä ja haittoja mietitään luvussa 5. Luvussa 6 pohditaan, miten kyseistä aihetta voidaan tutkia tulevaisuudessa ja tutkielma loppuu lukuun 7, jossa on yhteenveto ylös nousseista aiheista.

2 Bottifarmit

Bottifarmit (engl. bot farms) ovat merkittävä osa nykyaikaista geopoliittista vaikuttamista. Tämä suhteellisen uusi teknologian käyttötapa ilmestyi sosiaalisen median syntymisen kautta ja laajentui samalla, kun sosiaalisen median käyttö kasvoi. Ne hyödyntävät sosiaalisille medioille luotua toimintalogiikkaa, jossa palveluntarjoajat haluavat pitää käyttäjiä alustoillaan mahdollisimman kauan. Tämä tehdään julkaisemalla ja jakamalla bottiverkoston kanssa sisältöä, jota bottifarmin ylläpitäjä haluaa levittää palveluissa. Keskeinen tavoite näille bottifarmeille on rakentaa narratiivi, joka vaikuttaa sosiaalisten medioiden käyttäjien päätöksiin sekä mielipiteisiin. Tässä luvussa määritetään bottifarmien käsite ja tutkitaan, millä tavoin näitä bottifarmeja käytetään vaikuttamiseen sosiaalisissa medioissa.

2.1 Bottifarmit yleisesti

Bottifarmit ovat kokonaisuuksia, jotka muodostuvat automatisoiduista käyttäjätileistä, niitä yhdistävästä ohjelmistosta sekä eri infrastruktuureista riippuen siitä, miten bottia ylläpidetään. Tämä infrastruktuuri erottelee farmit toisistaan, sillä niiden toteutus voi perustua erilaisiin teknisiin ratkaisuihin sen perusteella. Farmit voivat esimerkiksi muodostua yhdestä keskuspalvelimesta, joka hallitsee käyttäjiä samalta laitteelta. Alhaisten kustannuksien vuoksi bottifarmit voivat muodostua myös lukuisista mobiililaitteista, joita automoidaan eri ohjelmistojen avulla. Harvinaisempi

tapa muodostaa näitä farmeja on verkossa käyttäen pilvipalvelu ympäristöjä järjestelmän hallintaan.

Bottifarmien keskeisin tavoite on vaikuttaa sosiaalisissa medioissa niille määritetyillä tavoilla. Tämä tehdään luomalla palveluihin valeprofileja, jotka julkaisevat tavoitteeseensa liittyvää sisältöä ja jakavat samanlaista, yleisesti toisten bottien luomaa sisältöä. Toisin kuin yksittäiset botit, bottifarmit toimivat yhtenäisesti sosiaalisissa medioissa, jolloin jokaisella botilla on oma roolinsa vaikutuksessa. Niiden julkaisut ovat hyvin koordinoituja, ja niitä julkaistaan juuri sopiviin aikajaksoihin, jolloin käyttäjämäärä on suurimmillaan. Tykkäykset ja jakamiset muilta boteilta tehdään myös räjähdysmäisesti, jotta sosiaalisten medioiden algoritmit jakaisivat niitä eteenpäin. Bottifarmit voivat myös koostua pelkästään käyttäjistä, joiden tehtävänä on jakaa oikeiden ihmisten julkaisuja (Shao ym., 2018). Tällaisissakin tilanteissa jaetut julkaisut yleisesti koostuvat äärisisällöstä, jonka lopputavoitteena on joko levittää tätä sisältöä tai tienata käyttäen sosiaalisten medioiden mainospalveluiden kautta.

Sosiaalisen median alustat perustuvat algoritmeihin, jotka yrittävät pitää käyttäjän sitoutumisen mahdollisimman kauan. Algoritmit ovat optimoituja siten, että ne saavat käyttäjän huomion mahdollisimman pitkäksi aikaa, mikä usein tehdään herättämällä heissä mahdollisimman voimakkaita tunteita. Käyttäjille esitellään tämän vuoksi laajoja määriä negatiivisia ja polarisoivaa sisältöä, sillä ne saavat eniten tykkäyksiä, kommentteja ja jakoja näissä palveluissa. (Brady ym., 2017) Bottifarmeissa olevat botit käyttävät tämän vuoksi julkaisuissaan tarkoituksellisesti jakavaa ja provosoivaa tekstiä, jotta niitä jaettaisiin enemmän (Stella ym., 2018).

Botit eroavat negatiivisen teeman lisäksi myös muin tavoin keskivertokäyttäjistä. Ne jakavat julkaisuja enemmän kuin kirjoittavat niitä, mikä auttaa niitä välttämään mahdolliset tunnistusalgoritmit ja pitävät aiheen uskottavana. Lisäksi botit käyttävät enemmän kielellisesti johdonmukaisia rakenteita lauseissaan, sillä suoria sanamuotoja ja lauserakenteita käyttäessään botit välttävät mahdollisia semanttisia

virheitä. Botit myös lisäävät julkaisuihinsa paljon enemmän aihetunnisteita (engl. hashtag), jonka tavoitteena on levittää viestiä enemmän halutuille ihmisryhmille. Botit keskittyvät yleisesti vain ajankohtaisiin ja suosittuihin aiheisiin, toisin kuin ihmiskäyttäjät, joiden julkaisut ovat yleisesti monipuolisempaa. (Ng & Carley, 2025), (Shao ym., 2018) Näiden kaikkien piirteiden päätavoite on samanaikaisesti lisätä bottien huomaamattomuutta niitä tunnistaville algoritmeille ja niiden huomattavuutta varsinaisille käyttäjille.

Vaikka termit ovat samankaltaisia, bottifarmit eivät ole bottiverkkoja. Bottiverkot muodostuvat haittaohjelmilla kaapatuista laitteista tai käyttäjistä, joiden avulla laitteita hallitseva bottimestari (engl. botmaster) käyttää näitä laitteita esimerkiksi palvelunestohyökkäyksiin (engl. DDoS), tietomurtoihin tai haittaohjelmien levitykseen. (Rataj, 2025) Bottifarmit taas muodostuvat tarkoituksellisesti niitä varten valmistetuista laitteista tai ohjelmistoista, joita käytetään yleisimmin vain vaikuttamiseen sosiaalisissa medioissa. Bottifarmien ja bottiverkkojen erottelu omiin ryhmiinsä on tärkeää, kun niiden erillisiä vaikutuksia ja mahdollista torjumista halutaan tutkia ja edistää.

2.2 Käyttötarkoitukset ja menetelmät

Bottifarmien käyttötarkoitukset vaihtelevat poliittisesta ja sosiaalisesta vaikuttamisesta eri taloudellisiin tarkoituksiin, mutta pohjimmiltaan ne perustuvat ihmisten sosiaalisten medioiden käyttötapoihin. Nyky-ihteiskunnassa sosiaalisen median käyttö on laajalle levinnyttä, ja tämä käyttö on vieläkin yleisempää teollistuneissa valtioissa, kuten Euroopassa (Euroopan unioni, 2024a). Sosiaalisen median käyttäjien määrän ennakoitaan kasvavan vieläkin enemmän lähivuosina, jolloin sen tärkeys informaatiolähteenä kasvaa. Bottifarmit haluavat muuttaa näissä alustoissa olevaa informaatiiovirtaa ja siten vaikuttaa käyttäjien ajattelutapaan ja käyttäytymiseen.

Poliittisen keskustelun heikentäminen on bottifarmien selvin ja tunnetuin käyttöaihe, erityisesti ylinegatiivisten viestien ja julkaisujen luomisen ja jaon kautta. Tämä vähentää varsinaista keskustelua aiheesta ja luo mielipiteiden välistä vastakkainasettelua. Tällaista yhteenottoa tapahtui esimerkiksi Katalonian kriisissä vuonna 2017, kun itsenäisyysäänestyksen yhteydessä botteja käytettiin provosoimaan ja yllyttämään niitä, jotka halusivat itsenäistyä, mutta myös niitä, jotka halusivat jäädä osaksi Espanjaa. (Stella ym., 2018) Botit eivät tukeneet yhtä puolta toisen sijasta, vaan esittivät olevansa molempien mielipiteiden puolesta puhuvia käyttäjiä. Näiden bottien lopullisena tarkoituksena oli lisätä poliittisten puolien välistä konfliktia ja heikentää luottamusta julkiseen keskusteluun.

Sosiaalisten medioiden algoritmeja voidaan hyväksikäyttää myös taloudellisin tavoin. Bottifarmeja on vuokrattavana sosiaalisen median sisäiseen mainontaan ja myynnin edistämiseen. Näistä palveluista voidaan ostaa tykkäyksiä, seuraajia, kommentteja ja muita algoritmia hyväksikäyttäviä markkinointitapoja. (Omena ym., 2019) Samalla tavalla kuin botit käyttävät algoritmia esittämään sen mukaan suosittuja julkaisuja uusille käyttäjille, nämä valekäyttäjät luovat keskustelua tuotteen ympärille, jolle bottifarmi on saanut ohjeita mainostaa. Reaaliaikainen keskustelu tuotteesta tekee siitä näennäisesti luotettavamman ostoksen, sillä bottien lähettämät julkaisut muistuttavat autenttisia käyttäjäkokemuksia ja arvioita.

3 Vaikutukset ja haitat

Vaikka bottifarmit sijaitsevat lähes täysin verkossa ja vaikuttavat laajasti vain sosiaalisten medioiden sisällä, niiden luomat vaikutukset näkyvät Euroopassa eri muodoissa. Tässä luvussa tarkastellaan bottifarmien aiheuttamia negatiivisia vaikutuksia ja niiden synnyttämiä yhteiskunnallisia haasteita.

3.1 Poliittinen manipulointi

Bottifarmien merkittävin vaikutusalue politiikassa. Bottien tekemä manipulaatio on kasvanut viime vuosina varsinkin vaalien ja suurten äänestysten yhteydessä. Näiden bottien lähettämien viestien ja jakamien julkaisujen määrä on kasvanut niin paljon, että niitä on todettu olevan lähes jokaisen länsimaisen äänestyskauden yhteydessä viime vuosina. Euroopan unionin tekemässä dokumentissa (Euroopan unioni, 2025a) mainitaan, että tällaisia todettuja vaikutustapauksia oli vuonna 2024 havaittu jopa 90:ssä eri valtiossa maailmanlaajuisesti. Näitä tapauksia todettiin 38 000 erillisessä kanavassa, lähes 25:llä eri alustalla, joiden yhteinen erillisten sisältöjen määrä oli 68 000.

Viime vuosina Euroopan alueella selvästi suurin vaikutuskohde on ollut Ukraina (Euroopan unioni, 2025a). Tämä manipulaatio kasvoi merkittävästi Venäjä-Ukrainan sodan alettua vuonna 2022. Botit olivat levittäneet propagandaa Ukrainan taistelukykyyn liittyen, jonka haluttu tulos oli heikentää ukrainalaisten taistelukykyä ja moraalia sodan suhteen. Lisäksi botteja käytettiin heikentämään länsimaista

tukea Ukrainaa kohtaan ja tukemaan Euroopan unionin vastaisia puolueita, joiden oletettiin suhtautuvan kriittisemmin Ukrainaa kohtaan. Maailmanlaajuisella skaalalla botteja on käytetty muokkaamaan kansainvälisiä mielipiteitä Venäjän eduksi, myös sodan ulkopuolella. (Dryzhakova, 2025) Ukrainan tilanne kertoo, miten bottifarmit voidaan käyttää osana laajempaa informaatiovaikuttamista ja hybridisodankäyntiä varsinaisen sodankäynnin ohella. Kansalaisten moraali on tärkeää sodankäynnissä ja sen tuomien huolien estämisessä, jonka vuoksi sitä on pyritty heikentämään eri tavoilla. Bottifarmit voivat toimia monikäyttöisinä vaikuttamisvälineinä, joita voidaan käyttää uhrivaltion lisäksi myös kansainvälisen tuen heikentämiseen.

Muualla maailmassa näitä vaikutuksia löydetään lähes kaikissa merkittävässä vaaleista, varsinkin Euroopan alueella. Manipulaation määrä on Ukrainaa lukuun ottamatta lähes verrannollinen valtioiden väkilukuun verrattuna, jotta disinformaation määrä ei hukuta varsinaista keskustelua, eikä myöskään ole liian vähäistä. Vaikutusyrityksiä oli paikallisista vaaleista laajoihin äänestyksiin, kuten europarlamenttivaalit tai Yhdysvaltain presidentinvaalit. Botteja ja niiden tekemiä kommentteja löydettiin aikaisemmin mainituissa Katalonian itsenäisyysäänestyksissä, jossa valekäyttäjät esittivät itsenäisyyttä haluavia ja unionisteja, yrittäen levittää negatiivisuutta. Ne levittivät myös valeartikkeleita vuosien 2016 ja 2020 presidentinvaaleissa, lisäten polarisointia demokraattien ja republikaanien välillä. Tällaisia vaikutuksia on tapahtunut myös nykyvuosina, kun bottifarmit käytettiin vuoden 2024 Euroopan parlamentin vaaleissa tukemaan EU-vastaisia poliitikkoja ja myöhemmin kyseenalaistamaan näiden vaalien tulosten luotettavuutta. (Euroopan unioni, 2025a; Omena ym., 2019; Shao ym., 2018)

Bottien keskeisin tavoite on vaikuttaa kansalaisten ääniin vaaleissa, joko ohjaimalla käyttäjiä äänestämään äärikandidaatteja ja -puolueita, tai yleisesti välttämään maltillisten poliitikkojen tukemista. Bottifarmit luovat vääristyneitä käsityksiä julkisesta mielipiteistä mainostamalla haluamaansa poliittista aihetta. Tämä nostaa

äänestäjien kynnystä etsimään tietoa aiheesta ja edistää sen tukemista vain sen vuoksi, että aihe vaikuttaa olevan suosittu. Haluttu lopputulos tällaiselle vaikuttamiselle on heikentyvä poliittinen ajattelu, kasvava polarisaatio ja vahingoittuneet demokraattiset arvot (Euroopan unioni, 2025a).

3.2 Sosiaaliset haasteet

Bottifarmien toinen vakava uhka on sen tuomat vaikutukset yhteiskunnalliseen yhtenäisyyteen, joka ilmenee usein haluttuna sivuvaikutuksena yllä olevasta poliittisesta vaikutuksesta. Joissain tilanteissa kuitenkin botteja ei käytetä vain yhteen tiettyyn poliittiseen tarkoitukseen, vaan niiden tavoitteena on yhteiskunnan arvojen yleinen heikentäminen (Stella ym., 2018). Jotta bottien haluamaa aihetta levitettäisiin sosiaalisissa medioissa, sen pitää herättää voimakkaita tunteita. Tällaisen, yleisesti negatiivisen ja hyökkäävän sisällön ympärille ilmestyy keskustelua, kun alustan muut käyttäjät kommentoivat asiaa. Kun polarisoivaa sisältöä jaetaan jatkuvasti, se muokkaa alustan ilmapiiriä, jolloin lopulta varsinaisten käyttäjien välinen viestintä aggressiivisoituu ja polarisoituu laajasti.

Käyttäytymisen heikentyminen vahvistuu entisestään sosiaalisissa medioissa olevien yleisten ilmiöiden, kuten tietokuplien (engl. filter bubbles) kautta. Tietokuplat ovat yksittäisen käyttäjän ympärille muodostunut yhtenäinen näkymä, joka on muodostunut hänen ympärilleen selatessaan sosiaalisia medioita (Tamilina ym., 2024). Tämä näkymä on usein vääristynyt, sillä algoritmit suosittelevat käyttäjälle vain sisältöä, joka vastaa hänen kiinnostuksensa kohteita. Kun käyttäjä altistuu pelkästään yhdenlaiselle sisältötyypille, se luo hänelle virheellisen käsityksen aiheen suosiosta ja varmuudesta. Käyttäjän on vaikea tutkia kiinnostuksenaiheensa pätevyyttä, jos hänen sosiaalinen piirinsä alustojen sisällä on täysin samaa mieltä asiasta. Bottifarmit hyväksikäyttävät näitä kuplia jakaessaan valesisältöä verkossa ja muuntavat sisällönsä muotoon, joka näytettäisiin kaikille tietyissä tietokuplissa oleville (Euroopan

unioni, 2025a). Vakavimmissa tilanteissa käyttäjille on vaikeaa ymmärtää ja tulla toimeen muiden ihmisten kanssa, jotka eivät jaa samoja mielipiteitä hänen kanssaan. Tietokuplien ulkopuolisen näkemyksen nähdään virheellisinä tai vihamielisinä, ja tällainen sosiaalisen median sisällä oleva käyttäytyminen voi siirtyä palveluiden ulkopuoliseen vuorovaikutukseen.

Viime vuosina bottifarmit ovat kohdistaneet toimintaansa erityisesti eurooppalaisten kansalaisten luottamukseen heidän omia instituutioitaan kohtaan. Botit levittävät sisältöä, jossa kritisoidaan hallituksia, budjetteja ja poliittista johtoa. (Euroopan unioni, 2025a) Lopullisena tavoitteena tälle vaikutukselle on heikentää kansalaisten luottamusta poliittisen johdon päätöksiin ja vähentää virallisten tiedonlähteiden käyttöä, joka lisää kansalaisten tiedonkeruuta muista lähteistä, kuten sosiaalisista medioista. Vuonna 2020 alkaneen COVID-19-taudin aiheuttaman karanteenin aikana botteja käytettiin laajasti jakamaan disinformaatiota eri sosiaalisen median alustoilla. Väärää tietoa taudin rokotteista ja taudin luonteesta jaettiin lukuisilla valekäyttäjillä, minkä kautta rokotevastaisuus nousi suosiossa länsimaissa. Karanteenin alusta vuonna 2020 vuoteen 2023 kestäneessä tutkimuksessa tutkittiin 1,7 miljoonaa julkaisua Twitterissä/X:ssä, joista noin 22 prosenttia oli bottien tuottamia. Samanaikaisista ulkopuolisista aiheista vain 11 prosenttia oli keinotekoisia, mikä viittaa siihen, että botteja oltiin hyödynnetty erityisesti tautiin liittyvän disinformaation levittämiseen (Unlu ym., 2025). Kampanjalla oli pitkäkestoiset vaikutukset kansalaisten luottamukseen heidän omiin instituutioihinsa, ja nämä vaikutukset ovat säilyneet karanteenien lopun jälkeen.

3.3 Taloudellinen sabotointi

Bottifarmeja käytetään poliittisen ja sosiaalisen manipuloinnin lisäksi myös taloudelliseen vaikutukseen. Niitä voidaan käyttää taloudelliseen hyötymiseen, mutta myös eri markkinoiden horjuttamiseen laajalla kaavalla. Sosiaalisen median yleinen käyttö

on kasvamassa maailmanlaajuisesti, ja on jo hyvin suosittua Euroopan alueella (Euroopan unioni, 2024a). Koska suurin osa Euroopan väestöstä käyttää näitä sivustoja, ne ovat myös tärkeitä markkinointialustoja. Sosiaalisissa medioissa mainostaminen ei riipu aikarajoista tai päivän ajankohdista, sillä sovelluksia käytetään täyspäiväisesti ja mainoksia voidaan sijoittaa suoraan käyttäjien sisältövirtoihin. Mainosjulkaisun levinneisyys riippuu siitä, kuinka monelle tämä julkaisu saadaan jaettua, johon bottifarmit ovat täydellisiä. Julkinen mielipide ja suosio ovat sosiaalisissa medioissa tärkeitä markkinoinnin työkaluja. Keskustelu tuotteesta tai brändistä on itsessään mainontaa näillä alustoilla, jonka vuoksi suosiolla ja seuraajilla voi olla laajat vaikutukset mainoskampanjan onnistumiseen näillä alustoilla. Bottifarmeja voidaan käyttää luomaan keinotekoista kuvaa suosiosta seuraamalla tilejä, jakamalla sisältöä ja luomalla keskustelua tuotteiden ympärille. Verkossa on palveluita, joihin maksamalla asiakkaat voivat ohjata näillä sivustoilla suuria joukkoja bottikäyttäjiä mainostamaan asiakkaan haluamia käyttäjiä ja julkaisuja. (Omena ym., 2019) Tämä toiminta aiheuttaa kuitenkin merkittäviä haasteita markkinaympäristölle. Kun seuraajat ja tykkäykset eivät aina ole todellisia, se tekee kilpailusta erittäin vaikeaa niille, jotka yrittävät rehellisesti myydä tuotteitaan. Vaikka boteilla tehty suosio on keinotekoista, se toimii silti algoritmeille, ja niiden sisältöä suositellaan laajemmalle käyttäjäjoukolle.

4 Eurooppalaisen kyberturvallisuussektorin kehitys ja yhteistyö

Bottifarmien ja muiden vastaavien teknologisen kehityksen synnyttämien uhkien lisääntyessä monet valtiot turvautuvat yhteisöihin, kuten Euroopan unioniin, turvaamaan kansalaisiaan parhaansa mukaan näiltä uhilta. Samanlaisia sääntelyitä ja strategioita tehdään myös valtio- ja alustakohtaisella tasolla. Ulkopuolisen manipulaation kasvaessa sosiaalisissa medioissa näiden torjuntakeinojen on merkitys kasvaa ja niitä joudutaan jatkuvasti vahvistamaan, jotta ne suojelisivat eurooppalaisia paremmin koko ajan muuttuvassa digitalisessa ympäristössä. Tässä kappaleessa tarkastellaan eri tapoja, joilla yksittäisissä eurooppalaisissa maissa ja Euroopan unionissa on valmistauduttu torjumaan näitä ulkopuolisia uhkia.

4.1 Sääntely ja lainsäädäntö

Ennen bottien tekemään manipulaatiota sosiaalisissa medioissa, Euroopan valtioilla oli omia valtiokohtaisia säädöksiä, jotka torjuivat yleisesti ihmisten tekemää tahallista manipulaatiota. Esimerkiksi Ranskassa säädettiin vuonna 2018 lakeja, joiden avulla voitiin tarkkailla verkossa olevaa sisältöä disinformaation varalta. Saksassa puolestaan säädettiin vuonna 2017 voimaan NetzDG:n (engl. Network Enforcement

Act), joka pakotti laajat sosiaaliset mediat poistamaan laittomat julkaisut sakon uhalla alustoiltaan. Nämä säädökset olivat kuitenkin alkeellisia eivätkä olleet tarpeeksi kattavia suojatakseen kansalaisia laajoilta manipulaatiokampanjoilta, jotka myöhemmin yleistyivät sosiaalisissa medioissa. Bottifarmien ja digitaalisen manipulaation nopeasta kasvusta huolimatta varsinkin Euroopan unioni on reagoinut aktiivisesti niiden tuottamiin uhkiin. Viimeisen vuosikymmenen aikana on säädetty useita koko unionin laajuisia lakeja ja säädöksiä, joita on otettu käyttöön torjumaan bottien harjoittamaa informaatiovaikuttamista.

Yhtenä Euroopan unionin ensimmäisistä säädöksistä tämänlaisen manipulaation sääntelyyn on tekoälysäädös (engl. AI Act), joka luokittelee eri tekoälyn käyttötarkoituksia omiin riskialueisiinsa, joista pitää joko ilmoittaa, tarkkailla tai kieltää kokonaan. Tekoälyllä tehty vaikuttaminen asetettiin tämän säädöksen kautta suurimpaan riskiryhmään, joka kieltää sen kokonaan Euroopan unionin alueella. Samanlaisen arvion sai esimerkiksi eri sosiaalipisteytysmekaniikat ja tietoturva-aukkojen hyväksikäyttö tekoälyn kanssa. Säädos velvoittaa tämän lisäksi, että generatiivisella tekoälyllä tehdyn sisällön pitää sisältää tiedon siitä, että se on keinotekoisesti tehty, eikä oikean ihmisen tekemä. (Euroopan unioni, 2024b) Koska bottifarmien toiminta perustuu siihen, että ne jäljittelevät ihmiskäyttäjien toimintaa, säädos tekee niiden toiminnasta täysin lainvastaista Euroopan alueella. Tekoälysäädös oli yksi ensimmäisiä tekoälyä sääteleviä laajan yhteisön tekemiä säädöksiä, mikä kertoi bottifarmien ja tekoälyn luoman uhkan lisäksi myös Euroopan unionin valmiudesta torjua näitä uhkia.

Tekoälysäädöksen lisäksi Euroopan unionin alueelle vaikuttavia bottifarmeja vahtii digipalvelusäädös, (engl. Digital Services Act, DSA) joka yrittää käyttäjien yleisen turvallisuuden ylläpitämisen ohella varmistaa, että sosiaaliset mediat tekevät säännöllisiä tutkimuksia sivujensa ja sovelluksiensa sisältöön. Säädos velvoittaa yritykset vähentämään ja ehkäisemään kyseistä manipuloivaa tekstiä ja näitä levit-

täviä käyttäjiä. Digipalvelusäädöstä käyttäen Euroopan Unionin jäsenvaltiot voivat valvoa tarkemmin, minkälaista sisältöä nämä valekäyttäjät levittävät. Lisäksi säädös antaa jäsenvaltioille oikeuden sakottamaan palveluntarjoajia, jos heidän mielestään alusta ei tee tarpeeksi vähentääkseen poliittisesti manipuloivaa valesisältöä heidän sivustoiltaan. (Euroopan unioni, 2022)

Näitä lakisäännöksiä päivitetään ja laajennetaan jatkuvasti suojelemaan eurooppalaisia uusilta uhilta, jotka kohdentuvat heihin. Vuonna 2024 muodostettiin Euroopan unionin sisäinen järjestö EUDS (European Democracy Shield), jonka tehtävänä on ylläpitää ja vahvistaa demokraattisia arvoja ja tasa-arvoisia vaaleja Euroopan alueella. Marraskuussa 2025 he julkaisivat joukon uusia eri toimenpiteitä, joihin sisältyi muun muassa päivityksiä aikaisemmin mainittuun digipalvelusäädöksen tekoällysisällön tulkintaan, erityisesti tekoälyn tekemään sisältöön vaaliprosesseissa ja muussa poliittisessa vaikutuksessa. (Euroopan unioni, 2025d)

4.2 Turvastrategiat ja suojautuminen

Bottifarmipuolustus on vain yksi osa kokonaisuutta, joka torjuu eri hybridiuhkia Euroopassa (Kalniete & Pildegovičs, 2021). Tämänlainen eurooppalainen turvautuminen ulkopuolisiin hyökkäyksiin perustuu lukuisiin monikansallisesti kehitettyihin strategioihin. Yleisen keskustelun manipuloinnin vähentämiseksi käytetään yllä mainittujen lainsäädäntöjen lisäksi eri teknisiä, yhteiskunnallisia ja koulutuksellisia keinoja, joiden tavoitteena on heikentää bottifarmien vaikutuksia Euroopassa. Näiden toimien ylläpidosta ja koordinoinnista vastaa joukko valtioita ja laajoja yhteisöjä.

Julkisen keskustelun manipulaation tunnistaminen on moniutkaista ja vaatii usein ylimääräistä kontekstia. On tärkeää erottaa, onko kyseessä yksittäistä keskustelua politiikan äärialueella, vai laaja yhteiskuntatasoinen ja koordinoitu operaatio. Resurssien käyttö satunnaisiin alueisiin vähentää niiden käyttöä laajoihin vaikuttamisoperaatioihin, jonka vuoksi selvät ominaisuudet tällaiselle manipulaatiolle ovat

tärkeässä asemassa. Vuonna 2023 Euroopan ulkosuhdehallinto (engl. European External Action Service, EEAS) luokitteli ensimmäistä kertaa laajat Euroopan ulkopuolelta tulevat vaikutusyritykset nimityksellä FIMI (engl. Foreign Information Manipulation and Interference). FIMIt ovat käyttäytymismalleja sosiaalisissa medioissa, joissa toistuu tahallinen ja koordinoitu sisältö, jonka tavoitteena on manipuloida käyttäjiä. Nämä FIMIt ovat myös usein kansainvälisiä, jolloin niitä luodaan Euroopan alueen ulkopuolella, mutta käsittelevät silti eurooppalaisista aiheita tai sellaisia aiheita, jotka vaikuttavat eurooppalaiseen elämään. Näiden luokitusten kautta hyökkäyksiä on voitu tutkia ja tarkastella paremmin (Euroopan unioni, 2025a). EEAS julkaisee vuosittaisesti raportin näistä FIMI-operaatioista, minkä kautta niiden leviämistä ja määrää voidaan verrata aikaisempiin vuosiin ja toimia sen mukaisesti.

Koska kaikkea vaikutusta ei voida torjua valtiotasolla, eurooppalaiset valtiot ovat pyrkineet kasvattamaan kansalaistensa kykyä arvioida tekstejä kriittisesti. Euroopan komissio on lähivuosina tukenut eri kampanjoita, joiden avulla pyritään edistämään medianlukutaitoa, lähdekriittisyyttä ja disinformaation tunnistamista (Euroopan unioni, 2020). Näitä kampanjoita keskitetään varsinkin nuorille johtuen heidän kasvavasta verkossa olostaan ja etäopiskelun yleistymisestä. Nuorilla on myös parhaat mahdollisuudet harjoittaa omaa lähdekriittisyyttään kouluissa ja muussa koulutuksessa, jonka vuoksi komissio on ohjannut eurooppalaisia kouluja tällaiseen koulutukseen. Koska sosiaalinen media koostuu pitkälti yksityisiä palveluita, jotka perustuvat algoritmeihin, käyttäjien on tärkeää suhtautua lukemaansa tietoihin kriittisesti sekä tutkia lukemiaan asioita.

4.3 Yhteistyö ja tiedonvaihto

Bottifarmien aiheuttamien uhkien laajuus ja nopea kasvu viime vuosina on vaatinut kasvavaa kansainvälistä yhteistyötä sen torjumiseksi. Yhteen koottu informaatio ja osaaminen antavat eurooppalaisille valtioille parhaimmat edellytykset estämään

manipulaatiota sosiaalisissa medioissa. Tätä varten monet eurooppalaiset valtiot tekevät yhteistyötä osallistumalla eri tiedonvaihtosopimuksiin ja järjestöihin. Tällainen yhteistyö tapahtuu hyvin usein EU-tasolla unionin läheisyyden vuoksi, mutta bottifarmien maailmanlaajuisuuden vuoksi sitä tehdään myös sen ulkopuolella. Eurooppalaiset NATO-valtiot tekevät ulkopuolisten NATO-jäsenten kanssa yhteistyötä disinformaation torjumiseksi, erityisesti Yhdysvaltojen kanssa.

Euroopan unionin tarkkailu perustuu lakisäädöksiin, joista tärkeimpiä mainittiin aikaisemmin. Lakimuutokset kieltävät bottifarmien käytön disinformaation levittämiseen EU:n, alueella, mutta näiden manipulaatioyritysten tarkkailuun on omat järjestönsä. Eurooppalainen digitaalisen median seurantakeskus (EDMO) on 28 eri eurooppalaisen valtion verkosto, jonka tehtävänä on tarkkailla ja tutkia disinformaatiota Euroopan alueella. Hanke yhdistää eri faktantarkistusyhtiöitä ja asiantuntijoita alalta, ja sen tekemät tutkimukset ovat erittäin tärkeitä edistämään bottifarmien vastaista kehitystä. EDMO tekee tiivistä yhteistyötä jäsenvaltioiden kanssa paikallisesti, tukien heitä disinformaation ja sen vaikutuksen rajoittamiseksi. (Euroopan unioni, 2025c) Euroopan kamppailu bottifarmeja vastaan ei kuitenkaan rajoitu pelkästään Euroopan alueelle. Sosiaalisen median manipulointia tapahtuu EU:n lisäksi myös Pohjois-Amerikassa, jolloin niiden kohteena on useimmiten Yhdysvallat, Kanada sekä muut NATO-valtiot (Euroopan unioni, 2025a).

5 Tekoälyn luomat hyödyt ja haitat

Marraskuussa 2022 yhdysvaltalainen yritys OpenAI julkaisi suuria kielimalleja käyttävän tekoälyn: ChatGPT:n, joka mahdollisti tekoälyn nousun 2020-luvulla. Tämän kehityksen myötä tekoälypohjaisia järjestelmiä alettiin hyödyntää myös informaatiovaikutuksessa, mukaan lukien bottifarmien toiminnassa ja myöhemmin myös bottifarmien vastaisessa toiminnassa. Tässä kappaleessa tarkastellaan, miten tekoälyn kehitykset tulevat vaikuttamaan bottifarmien käyttöön kansainvälisessä vaikutuksessa.

5.1 Skaalautuvuus ja personointi

Yksi bottifarmien suurimmista vahvuuksista on niiden kyky skaalautua helposti laajassa mittakaavassa vähäisellä infrastruktuurilla. Yhdessä verkostossa saattaa olla yhteydessä tuhansia automatisoituja käyttäjätilejä, jotka jakavat ja puhuvat samoista asioista sosiaalisissa medioissa. Laajojen bottifarmien ylläpito ilman tekoälyä on kuitenkin kallista tai vaikuttaa niiden vakuuttavuuteen, sillä alkeelliset botit eivät pystyneet helposti ajatella siitä, mitä ne julkaisivat ja levittivät internetissä. Jos manipulaatio haluttiin toteuttaa oikeilla ihmisillä, se vaati laajasti resursseja, joi- ta on vaikeampi kouluttaa, koordinoita ja ylläpitää. Generatiivinen tekoäly pystyy ohjeiden saatuaan työskennellä itsenäisesti tai moitteettomasti osana koordinoitua joukkoa. Ne ovat myös resurssikannalta paljon kustannustehokkaampia, kuin aikai-

semmat mallit, sillä ne eivät vaadi jatkuvaa ihmistoimijan läsnäoloa. (Lopez-Joya ym., 2025)

Generatiivisen tekoälyn valtavat kirjastot auttavat niitä myös mukautumaan niille annettujen ohjeiden mukaisesti. Tällaista tekoälyä käyttävät bottifarmien välekäyttäjät voivat helposti omaksua tiettyjä ihmispiirteitä ja ylläpitää niitä keskustellessaan sosiaalisessa mediassa, mikä tekee niistä hyvin uskottavia. Vuonna 2024 tehdyssä testissä ja sitä seuraavassa kyselyssä vain 42 prosenttia kokeeseen osallistuneista ihmisistä osasi erottaa eri LLM:eillä toimivat botit oikeista ihmisistä, joiden kanssa he olivat keskustelleet (Lopez-Joya ym., 2025). Tekoälyn kehittyessä tämä luku voidaan olettaa pienentyvän entisestään, jolloin jokapäiväinen bottien erotus oikeista ihmisistä heikkenee ja bottifarmien tärkeys manipulointityökaluna kasvaa.

5.2 Järjestelmät bottien tunnistamiseksi

Generatiivisella tekoälyllä toimivat botit käyttävät kontekstia keskusteluissa laajasti paremmin kuin aikaisemmissa malleissa, mikä piilottaa ne lähes kokonaan aikaisemmin botteja etsiviltä algoritmeilta. Vanhat algoritmit tunnistivat botteja muun muassa julkaisujen määrissä tietyissä aikajaksoissa ja sen sisältämässä tekstissä. Alkeelliset botit toimivat tietyillä algoritmeilla, jotka eivät osanneet ajatella lauseita, vaan julkaisivat valmiiksi tehtyjä tekstejä ilman niiden ulkopuolista interaktiota palvelun kanssa, jolloin niiden tunnistaminen oli helppoa. Uusimmat botit osaavat kommentoida, tykätä ja jakaa julkaisuja sosiaalisissa medioissa, jolloin näillä algoritmeilla on hyvin vaikeaa erottaa niitä oikeista käyttäjistä. Nopeasti muuttuvaa ja kehittyvää teknologiaa vastaan tarvitaan nopeasti parantuvia tunnistamistapoja, minkä vuoksi tekoälyä käytetään nykyään myös torjumaan ja tunnistamaan tällaista manipulaatiota sosiaalisissa medioissa.

LLM:ien mukautuvuus ja monikäyttöisyys tekee siitä monipuolisen työkalun laajojen bottioperaatioiden tunnistamisessa. Tuoreissa tutkimuksissa esitellään, kuin-

ka kielimallien valmiita kielivarastoja voidaan käyttää samoja kirjastoja käyttävien bottien tunnistamiseksi. Ohjelmistokehys LGB (engl. language model and graph neural network) yhdistää kielimallien kirjastot erilliseen neuroverkkoon, joka tunnistaa bottitutkia vältteleviä toimintoja (Zhou ym., 2025). Toinen samanlainen kehys on LMBot, joka tutkii kielimallin kanssa käyttäjiä ilman neuroverkkoa, tehden tunnistusprosessista tehokkaamman (Cai ym., 2024). LLM:iä voidaan mahdollisesti käyttää myös ketjussa, jolloin ne katsovat käyttäjätietojen alueita erikseen. Yksi tutkii käyttäjien metadataa, eli seuraajia, julkaisumääriä ja käyttäjien profileja. Toinen kielimalli taas tarkkailisi käyttäjän julkaisujen kirjallista tietoa, kuten mistä niiden viestit muodostuvat ja miten ne eroavat. Kolmas malli voisi taas vahtia käyttäjän yhteyksiä, kuten kenen kanssa käyttäjä on vuorovaikutuksessa, kuka seuraa käyttäjää ja mitä julkaisuja käyttäjä katselee. (Feng ym., 2024)

5.3 Bias ja disinformaatio generatiivisella tekoälyllä

Generatiivisen tekoälyn muutti ja tulee muuntamaan bottifarmien ja sosiaalisen median manipulointia täysin. Sen tuoma helppokäyttöisyys, muokattavuus ja adaptoituvuus tekevät tahallisesti pahansuovasta vaikuttamisesta yhä helpompaa. Generatiivisen tekoälyn käyttö antaa myös kyvyn tehdä deepfake-mediaa. Deepfake (engl. yhdistelmä sanoista deep learning ja fake) viittaa synteettisiin videoihin, kuviin ja äänitallennuksiin, jotka ovat joko täysin tai osittain tekoälyn generoimia. Näitä luomuksia voidaan tehdä kuvaamaan tapahtumia, joita ei ole tapahtunut oikeassa elämässä. (Fagni ym., 2021)

Deepfaket ovat siltä kannalta katastrofaalisia, että ne heikentävät luottavuutta mediaan. Mikä saattoi olla täysin varmaa informaatiota, ei enää ole. Kuvia ja videoita voidaan epäillä synteettisiksi, vaikka ne olisivat täysin oikeita, mikä heikentää keskustelun yleistä luottavuutta. Tekaistuja videoita voidaan myös esittää todellisina, ja jos tarpeeksi suuri määrä botteja jakaa niitä ja keskustelee niistä, ne voidaan

myös ymmärtää todellisena. Jaettujen deepfake-videoiden määrä on kaksinkertaistunut Euroopassa lähivuosina kuuden kuukauden välein, ja vuonna 2025 jaettujen tekaistujen videoiden määrä oletetaan lähestyvän 8 miljoonaa (Euroopan unioni, 2025b).

Disinformaation jakotavat eivät kuitenkaan lopu pelkästään bottifarmeihin ja valekäyttäjiin, vaan väärennettyä tietoa voidaan sijoittaa suoraan luotettuihin tietolähteisiin. Tekoälyn käytön kasvaessa sosiaalisissa medioissa esimerkiksi X:n Grok- tekoälyn tai Googlen Google Geminin kautta, kasvaa myös niiden tärkeys tiedonlähteinä. Tällaiset tekoälyavustajat käyttäjät käyttävät yleisesti laajoja kirjastoja ja tieteellisiä artikkeleita vastatessaan kysymyksiin, mutta tähän hakusisältöön voidaan vaikuttaa ulkoisesti. Tekoälyt etsivät oman datansa lisäksi myös verkosta sisältöä, jotta niiden vastaukset ovat mahdollisimmat tarkkoja ja oikeita, yleisesti myös riippumatta sivustosta, jolloin ne saattavat ottaa tietonsa hyvinkin biasoituilta sivustoilta. Pienikin määrä biasoitua tai väärennettyä sisältöä voi vaikuttaa tekoälyavustajien vastaukseen, ja tämä vaikutus suurenee kielimallien koosta riippuen (Bowen ym., 2025). Tarpeeksi koordinoidulla vaikutusoperaatiolla näistä avustajista voidaan tehdä laajoja disinformaation jakajia niiden omilla alustoilla.

6 Pohdinta

Tutkimuksista voidaan päätellä, että bottifarmien tarkat tulevat vaikutukset yhteiskuntaan ja sen käytöt tulevaisuudessa ovat vielä epäselviä. Bottifarmit ovat yleisesti tunnettuja asioita, mutta aiheen uutuuden vuoksi niille ei ole vielä tarkkaa laillista tai tieteellistä konseptia (Dryzhakova, 2025). Aiheeseen liittyviä ilmiöitä, kuten sosiaaliset botit, bottiverkkoja ja digitaalista disinformaatiota on tutkittu, joten niistä saa suuntaa-antavan idean bottifarmien tärkeydestä tulevaisuudessa. Bottifarmeja tulee kuitenkin tutkia enemmän tarkalleen niihin keskittyen, jotta niiden haittoja voidaan estää mahdollisimman tehokkaasti.

Toisaalta, tämänlaisen digitaalisen manipulaation rooli tulee kasvamaan katsoen maailmanlaajuisen diplomatian kehityssuuntaa lähivuosina. Maailmanlaajuisen luotto yksilön vapauksiin ja demokratiaan on heikentynyt suuresti ja auktoritaarinen ajattelutapa on noussut suosiossa (Freedom House, 2025). Tällaisissa hallinnoissa valvonta ja valehtelu on hyvin yleisempää, jonka vuoksi kansalaisten digitaalinen tarkkailu on kasvanut kaikkialla. Valtiotasoisilla bottifarmeilla voidaan luoda narratiivi, jonka kautta hallinnot voivat esittää kansalaisilleen mitä tahansa he haluavat ohjatakseen kansalaisten ajattelua ja vähentämään toisinajattelua.

Bottifarmien käyttö ja torjuminen tulee olemaan tärkeää myös lähitulevaisuuden maailmanlaajuisessa diplomatiassa. Suurin osa vuonna 2024 todettuja Eurooppaan kohdistettuja FIMI-hyökkäyksistä oli peräisin valtioista, joissa on auktoritaarinen hallitus, kuten Kiina ja Venäjä (Euroopan unioni, 2025a). Suurten yhteisöjen, ku-

ten NATOn ja YKn vaikutusvallan heikkeneminen tulee johtamaan siihen, että nämä valtiot voivat helpommin vaikuttaa muiden valtioiden sisä- ja ulkopoliittikkaan näin tavoin varsinaisen diplomatian sijasta. Vastapuolena kuitenkin, näiden bottifarmien ja digitaalisen manipulaation kasvaessa tulee nousemaan myös niiden vastaiset toimenpiteet. Euroopan unioni mainitsee keskittyvänsä jäsenvaltioidensa demokration ylläpitoon ja digitaalisen manipuloinnin estämiseen, ja tekee koko ajan uutta lainsäädäntöä ja tutkintoja disinformaation estämiseen sosiaalisissa medioissa (Euroopan unioni, 2020, 2025d).

Maailman poliittisesta tilanteesta huolimatta bottifarmien tärkein kasvattaja tulee selvästi olemaan generatiivinen tekoäly ja eri kielimallit. Niiden kyky muistuttaa ihmistä kokoaikaisesti ja niiden halpuus tulee muuttamaan bottiverkostojen rakennetta kokonaan, tehden niistä helppokäyttöisiä ja hyvin skaalattavia. Maailmanlaajuinen taloudellinen sijoitus uusien sekä parempien tekoälyjen kehitykseen, ja varsinkin kielimallien koulutukseen, tulee kasvattamaan tätä verkostorakenteiden muutosta entisestään. Tekoälyn käyttö tulee tulevaisuudessa tarvitsemaan laajoja säännöstelyjä, jotta sen vaikutus yhteiskunnan vakauteen voidaan minimoida.

7 Yhteenveto

Tutkimuksessa tutkittiin bottifarmeja konseptina ja etsittiin niiden aiheuttamia hyötyjä ja haittoja Euroopassa. Lisäksi tarkasteltiin, miten tavoin eurooppalaiset valtiot ovat lyhyen aikajakson aikana kehittyneet torjumaan bottifarmeja ja muita hybridisodankäynnin työkaluja. Lopuksi tutkittiin, miten tavoin tekoälyn kehitys lähi-vuosina on vaikuttanut ja tulee vaikuttamaan bottifarmien käyttöön ja torjuntaan sosiaalisessa mediassa.

Tutkimuksessa esitettyihin tutkimuskysymyksiin saatiin seuraavat vastaukset:

TK1: Millaisia haittoja bottifarmit aiheuttavat Euroopassa? Bottifarmien tutkinta sai selville, että bottifarmeilla on nousevat ja laajat negatiiviset vaikutukset moneen yhteiskunnan eri alueeseen. Botteja käytetään vaikuttamaan käyttäjien poliittisiin ja sosiaalisiin mielipiteisiin jakamalla heille laajoin määrin disinformaatiota. Tämän kaiken lopputavoitteena on saada käyttäjät äänestämään omia etujaan vastaan, luottoa demokraattisiin järjestelmiin ja vahingoittaa eurooppalaisten yhteiskuntien vakautta. Sosiaalisten medioiden algoritmien takia ja usein myös tahallisesti, bottien lähettämä sisältö on usein aggressiivista ja tunteita herättävää, jotta se leviää mahdollisimman monelle käyttäjälle. Tämä käyttäytyminen vahingoittaa alustojen keskustelun kohteliaisuutta ja luo polarisaatiota eri mielipiteiden välille, mikä saattaa levitä sosiaalisten medioiden ulkopuolelle. Bottifarmit toimivat myös taloudellisena palveluna, jolloin niitä käytetään luomaan keinotekoista keskustelua tuotteen tai käyttäjätilin ympärille eräänlaisena mainostamistapana.

TK2: Miten Euroopan kyberturvallisuussektori on kehittynyt bottifarmien torjuntaan? Eurooppalaiset valtiot ovat kehittäneet hybridisodankäynnin laajuuden vuoksi lukuisia eri säädöksiä ja lakeja, joiden tavoitteena on rajoittaa disinformaatiota sosiaalisissa medioissa vaalikausilla ja niiden ulkopuolella. Esimerkki näistä säädöksistä on tekoälysäädös, joka sääntelee tekoälyn käyttöä eri kehyksiin ja kieltää tietyt tekoälyn käyttötavat, mukaan lukien bottifarmeissa käytettävät valeprofiilit. Toinen esimerkki on digipalvelusäädös, joka velvoittaa sosiaaliset mediat torjumaan alustoilla olevaa disinformaatiota. Torjuakseen bottifarmit ja muu disinformaatio, eurooppalaiset valtiot tekevät yhteistyötä toistensa sekä ulkopuolisten maiden kanssa. Keskeisin tällainen eurooppalainen järjestö on EDMO, jonka yhteistyö keskittyy disinformaation tunnistamisen tutkimiseen ja ohjeiden levittämiseen toimimalla läheisesti paikallisten hallintojen kanssa.

TK3: Miten tekoäly on vaikuttanut bottifarmien toimintaan, ja miten sen rooli kehittyy tulevaisuudessa? Bottifarmien sisäinen infrastruktuuri on vaihtunut laajasti käyttämään generatiivista tekoälyä sen nopean kehityksen yhteydessä. Syy nopeaan vaihtoon lienee kielimallien skaalautuvuudessa ja helpossa personoinnissa, minkä kautta niitä on halpaa ylläpitää ja ohjata levittämään haluttua sisältöä sosiaalisissa medioissa. Tekoäly on myös lisännyt disinformaation luotettavuutta deepfake-medioiden avulla, jonka kanssa voidaan luoda hyvin todenmukaisia videoita, kuvia ja äänityksiä tukemaan bottifarmien digitaalista manipulointia. Tämä teknologia vähentää oikeiden videoiden, kuvien ja äänityksien luotettavuutta, jonka kautta yleinen luotto tietoon alustoilla kärsii. Kielimalleja voidaan käyttää myös bottien tunnistamiseen päivityksenä vanhoihin tunnistusjärjestelmiin, jotka eivät erota uusia botteja oikeista käyttäjistä.

Kaiken kaikkiaan todettiin, että bottifarmeilla on laajat uhkat eurooppalaiselle yhteiskunnalle, jotka tulevat hyvin varmasti kasvamaan tulevaisuudessa. Tämän uhan torjuminen tulee yhä tärkeämmäksi sosiaalisen median tärkeyden kasvaessa, jon-

ka vuoksi aihetta on syytä tutkia enemmän. Jatkotutkimuksissa voidaan tarkastella tällaisten bottifarmien tarkkaa laajuutta Euroopassa ja sen ulkopuolella. Lisäksi voidaan tutkia lisää tapoja tunnistaa valekäyttäjät oikeista käyttäjistä sosiaalisessa mediassa ja etsiä tapoja estää yhteiskunnan polarisoituminen näiden seurauksena.

Lähdeluettelo

- Bowen, D., Murphy, B., Cai, W., Khachaturov, D., Gleave, A., & Pelrine, K. (2025). Scaling trends for data poisoning in LLMs. *Proceedings of the Thirty-Ninth AAAI Conference on Artificial Intelligence and Thirty-Seventh Conference on Innovative Applications of Artificial Intelligence and Fifteenth Symposium on Educational Advances in Artificial Intelligence*. <https://doi.org/10.1609/aaai.v39i26.34929>
- Brady, W. J., Wills, J. A., Jost, J. T., Tucker, J. A., & Van Bavel, J. J. (2017). Emotion shapes the diffusion of moralized content in social networks. *Proceedings of the National Academy of Sciences of the United States of America*, 114(28), 7313–7318. <https://doi.org/10.1073/pnas.1618923114>
- Cai, Z., Tan, Z., Lei, Z., Zhu, Z., Wang, H., Zheng, Q., & Luo, M. (2024). LMBot: Distilling Graph Knowledge into Language Model for Graph-less Deployment in Twitter Bot Detection. *Proceedings of the 17th ACM International Conference on Web Search and Data Mining*, 57–66. <https://doi.org/10.1145/3616855.3635843>
- Dryzhakova, D. (2025). Legal regulation of the concept of “bot farms” as a response to manipulation of Internet users. *Social and Legal Studies*, 2(8), 144–154. <https://doi.org/10.32518/sals2.2025.144>
- Euroopan unioni. (2020). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and*

the Committee of the Regions On the European democracy action plan. Haettu 19. 05. 2026, osoitteesta <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:790:FIN>

Euroopan unioni. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) [Legislative Body: EP, CONSIL]. <http://data.europa.eu/eli/reg/2022/2065/oj>

Euroopan unioni. (2024a). *Digital society statistics at regional level*. Haettu 13. 05. 2026, osoitteesta https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_society_statistics_at_regional_level

Euroopan unioni. (2024b). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) [Legislative Body: CONSIL, EP]. <http://data.europa.eu/eli/reg/2024/1689/oj>

Euroopan unioni. (2025a). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*. Haettu 04. 11. 2025, osoitteesta <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf>

Euroopan unioni. (2025b). Children and deepfakes | Think Tank | European Parliament. Haettu 18. 11. 2025, osoitteesta [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2025\)775855](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)775855)

- Euroopan unioni. (2025c). *Eurooppalainen digitaalisen median seurantakeskus – ED-MO / Shaping Europe’s digital future*. Haettu 06. 12. 2025, osoitteesta <https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory>
- Euroopan unioni. (2025d). *European Democracy Shield and EU Strategy for Civil Society*. Haettu 24. 11. 2025, osoitteesta https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2660
- Fagni, T., Falchi, F., Gambini, M., Martella, A., & Tesconi, M. (2021). TweepFake: About detecting deepfake tweets [Publisher: Public Library of Science]. *PLOS ONE*, 16(5), e0251415. <https://doi.org/10.1371/journal.pone.0251415>
- Feng, S., Wan, H., Wang, N., Tan, Z., Luo, M., & Tsvetkov, Y. (2024). What Does the Bot Say? Opportunities and Risks of Large Language Models in Social Media Bot Detection. <https://doi.org/10.48550/arXiv.2402.00371>
- Freedom House. (2025). *The Uphill Battle to Safeguard Rights*. Haettu 08. 12. 2025, osoitteesta <https://freedomhouse.org/report/freedom-world/2025/uphill-battle-to-safeguard-rights>
- Kalniete, S., & Pildegovičs, T. (2021). Strengthening the EU’s resilience to hybrid threats. <https://journals.sagepub.com/doi/10.1177/17816858211004648>
- Lopez-Joya, S., Diaz-Garcia, J. A., Ruiz, M. D., & Martin-Bautista, M. J. (2025). Dissecting a social bot powered by generative AI: anatomy, new trends and challenges. *Social Network Analysis and Mining*, 15(1), 7. <https://doi.org/10.1007/s13278-025-01410-5>
- Ng, L. H. X., & Carley, K. M. (2025). A global comparison of social media bot and human characteristics. *Scientific Reports*, 15(10973). <https://doi.org/10.1038/s41598-025-96372-1>
- Omena, J. J., Chao, J., Pilipets, E., Kollanyi, B., Zilli, B., Flaim, G., Sívori, H., Ruiven, K., Rademakers, L., Li, M., & Nero, S. (2019). Bots and the black

- market of social media engagement. <https://doi.org/10.13140/RG.2.2.30518.52804>
- Rataj, P. (2025). Botnet defense under EU data protection law [Publisher: Elsevier Advanced Technology]. *Computer Law & Security Review*, 56, 106080. <https://doi.org/10.1016/j.clsr.2024.106080>
- Shao, C., Ciampaglia, G. L., Varol, O., Yang, K.-C., Flammini, A., & Menczer, F. (2018). The spread of low-credibility content by social bots. *Nature Communications*, 9(1), 4787. <https://doi.org/10.1038/s41467-018-06930-7>
- Stella, M., Ferrara, E., & De Domenico, M. (2018). Bots increase exposure to negative and inflammatory content in online social systems. *Proceedings of the National Academy of Sciences of the United States of America*, 115(49), 12435–12440. <https://doi.org/10.1073/pnas.1803470115>
- Tamilina, L., Hryniv, D., & Hulko, P. (2024). The Primary Predictors Behind the Formation of Social Bubbles on Online Social Media Platforms: Focusing on Young Individuals in Ukraine. <https://mp.ra.ub.uni-muenchen.de/121084/>
- Unlu, A., Truong, S., Sawhney, N., & Tammi, T. (2025). Unveiling the Veiled Threat: The Impact of Bots on COVID-19 Health Communication [Publisher: SAGE Publications Inc]. *Social Science Computer Review*, 43(4), 675–704. <https://doi.org/10.1177/08944393241275641>
- Zhou, M., Zhang, D., Wang, Y., Geng, Y.-a., Dong, Y., & Tang, J. (2025). LGB: Language Model and Graph Neural Network-Driven Social Bot Detection. *IEEE Transactions on Knowledge and Data Engineering*, 37(8), 4728–4742. <https://doi.org/10.1109/TKDE.2025.3573748>