TRAFICOM
Liikenne- ja viestintävirasto

Strateginen ennakointi

Kyberturvallisuuden skenaariot 2035

Traficomin teknologia- ja strategiatoiminto

Kyberturvallisuuden skenaariot 2035

Skenaarioraportin sisällysluettelo

Kyberturvallisuuden skenaariot 2035 - Taustaa

- **Kyberturvallisuuden skenaariot 2035** tukevat kyberturvallisuusstrategian poikkihallinnollisen kyberturvallisuuden tulevaisuus- ja ennakointityömallin rakentamista ja kyberturvallisuuden uhka-arvion luomista. Skenaariot rakennettiin aikavälillä syksy 2024 - kevät 2026.
- Mukana skenaariotyön eri vaiheissa on ollut monipuolisesti asiantuntijoita (200+) kyberturvallisuuskeskuksesta, yrityksistä, akatemiasta, kyberturvallisuuskeskuksen kv-vastinpareista, julkishallinnon toimijoista ja kansalaisyhteiskunnan edustajista.
- Kyberturvallisuuden skenaariot 2035 kuvaavat kyberturvallisuuden vaihtoehtoisia toimintaympäristöjä. Niiden kuvaamia maailmoja voidaan syventää ja jatkokehittää esimerkiksi **toimialatasoisessa tarkastelussa** ja käyttää **tulevaisuuslähtöisessä harjoittelussa**.
- Skenaarioita voidaan hyödyntää **organisaation varautumisen suunnittelussa** käyttämällä apuna tämän raportin liitteenä löytyviä **skenaariotyökaluja**.

Skenaarioilla käsitellään epävarmuutta

- Erilaiset toimintaympäristön avaintapahtumat vievät meitä tästä päivästä kohti **erilaisia tulevaisuuksia**. Emme vielä tiedä, minkälainen maailma on vuonna 2035, mutta **voimme yrittää varautua siihen hahmottamalla, mikä on mahdollista.**
- Kyberturvallisuuden skenaariot 2035 kuvaavat **ulkoisen toimintaympäristömme epävarmuuksien vaihtoehtoisia kehityskulkuja.** Ne toimivat systemaattisena tapana hahmottaa **erilaisia mahdollisia kyberturvallisuuden tulevaisuuksia.**
- Skenaariot ovat **vaihtoehtoisia tulevaisuuden päätöksenteon kontekseja, joihin eläytymällä voidaan tehdä ennakoiden parempia päätöksiä.** Ne auttavat ymmärtämään toimintaympäristön muutoksia kokonaisuutena, ennakoiden ilmiöiden keskinäisiä kytköksiä ja yhteisvaikutuksia.
- Skenaariot 2035 voivat nyt tuntua enemmän tai vähemmän mahdollisilta. **Maailma vuonna 2035 näyttää todennäköisesti eri skenaarioiden yhdistelmältä.**

Näin skenaariot rakennettiin

Muutostekijät

Kyselyissä, asiantuntijahaastatteluissa ja työpajoissa kartoitetut kyberturvallisuuden muutostekijät voivat kehittyä eri suuntiin ja tahtiin vuoteen 2035 mennessä.	
Geopoliittinen kehitys	AI & ML-kehitys
Digitaalinen infrastruktuuri	Kybersääntelyn tulevaisuus
Tulevaisuuden kyberuhat ml. rikollisuus	Informaatioympäristö ja yhteiskunta
Toimitusketjut	Kvanttiteknologia
EU:n yhtenäisyys ja asema	Teknologiajättien asema
Satelliitti- ja avaruusteknologia	Osaamisen kehitys
Organisaatioiden varautumisratkaisut	Tulevaisuuden haavoittuvuudet ja solmukohdat
Teknologiset riippuvuudet	Standardit ja luottamus
Kuluttajakäyttäytyminen	Disinformaatio ja hybridivaikuttaminen

Skenaarioiden muodostaminen

- Tiedonhakuvaiheessa toteutettiin sidosryhmien kanssa yhteensä neljä työpajaa, kaksi sidosryhmille kohdistettua skenaariokyselyä sekä 18 asiantuntijoiden teemahaastattelua.
- Skenaarioiden rakentamisvaiheessa toteutettiin sidosryhmien kanssa yhteensä neljä työpajaa sekä 4 asiantuntijoiden syventävää haastattelua.
- Skenaariot muodostettiin tulevaisuustaulukkomenetelmällä 8 vaikuttavimmasta tulevaisuuden muutostekijästä kehitysvaihtoehtoineen.

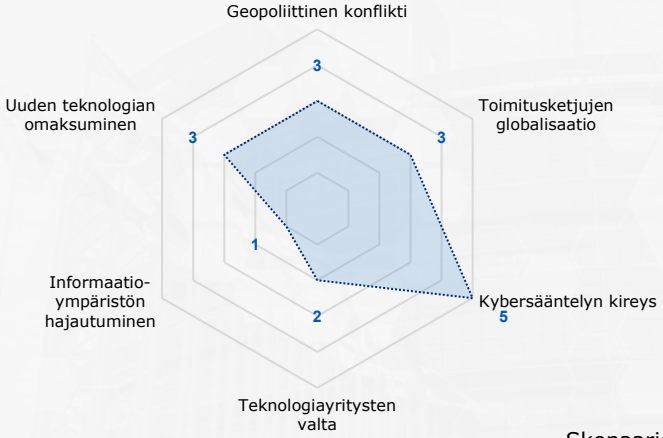
Skenaariokuvausten tasot

Kyberturvallisuuden skenaariot 2035 kuvaavat neljä vaihtoehtoista, mahdollista geopoliittisen ja teknologisen muutoksen värittämää maailmaa järjestelmineen, sekä tulevaisuuden maailmoissa mahdollisesti nousevia kyberuhkia ja haavoittuvuuksia.

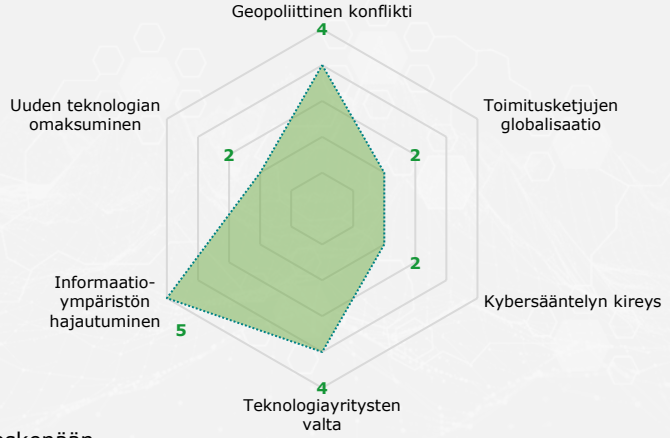
Kyberturvallisuuden skenaariot 2035

Skenaariokuvaukset

/TULENKANTAJA/

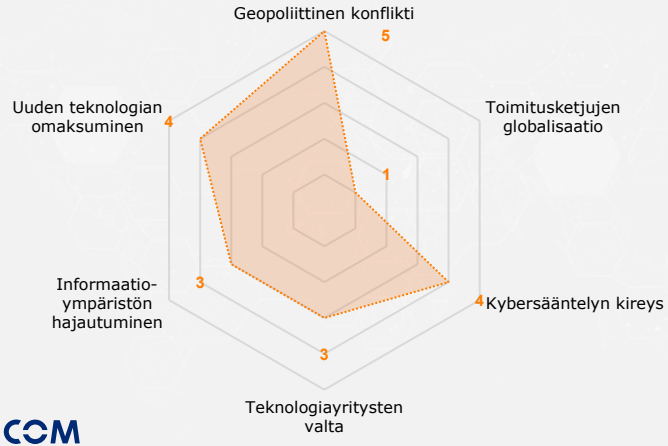


/PIRSTALOITUMINEN/

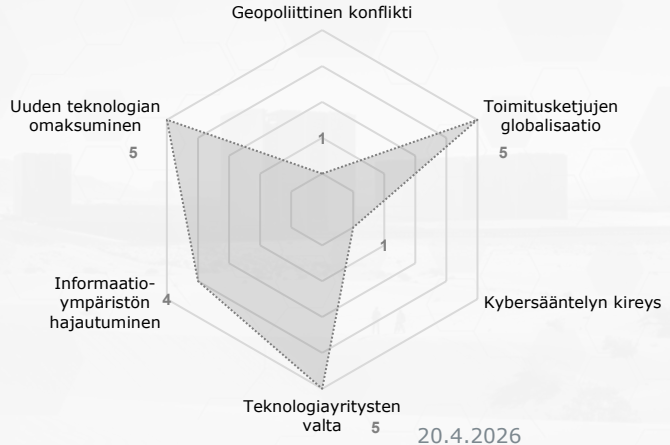


Skenaariot ovat piirteiltään erilaisia keskenään.
Siten ne toimivat parhaiten työkaluina uusien kyberturvallisuusilmiöiden tutkimiseen.

/KAKSI VALTAKUNTAA/



/DATAIMPERIUMIT/



TRAFICOM

/TULENKANTAJA 2035/

Vastakkainasettelu säilyy suurvaltojen etupiirien välillä.

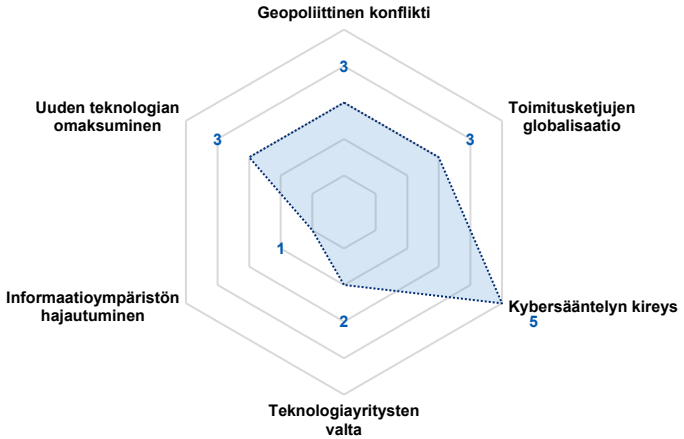
Yhdysvallat on säilyttänyt kansainvälisen johtoasemansa kilpakumppaniinsa Kiinaan nähden, mutta sisäiset haasteet ja ulkopoliittiset ylilyönnit ovat ajaneet sitä alati **autoritaarisemmaksi ja arvaamattomammaksi liittolaiseksi**. Nato-yhteistyö ja läntinen turvallisuusarkkitehtuuri on kuitenkin voimissaan, eikä **Kiina BRICS-liittolaisineen ole onnistunut haastamaan länsimaita menestyksekkäästi.** EU on kasvattanut strategista autonomiaansa suhteessa Yhdysvaltoihin, kantaen samalla oman kortensa kekoon demokratioiden liittoumassa. **Valtiotoimijat tiedustelevat ja sabotoivat länsimaiden järjestelmiä tulevia konflikteja ennakoiden.**

Uuden teknologian käyttöönotto on maltillista.

Tekoälykehitys ei ole lunastanut hurjimpia lupauksia ja suurimpia hankkeita on peruttu kannattamattomina. Infrastruktuurin ylirakentaminen, ratkaisujen ylimyynti, oikeusjutut ja tietomurrot ovat saaneet rahoittajat varovaisiksi, hidastaen käyttöönottoa ja johtaen suurien mallien tekoälytalveen. **LLM-kehityskaaren rinnalla onkin kehittynyt laadukkaaseen *luomudataan* ja rajattuihin käyttötapauksiin perustuvia AI-sovellutuksia** (mm. SLM-mallit ja reunalaiteratkaisut), jotka on otettu EU:ssa menestyksekkäästi käyttöön. Yhteismarkkinan laadukkaan yritysdatan yhteiskäytettävyys ottaa harppauksia. **EU on parantanut omavaraisuuttaan pilvipalveluissa, tekoälysovellutuksissa, sekä kvantti-, 6G-, ja avaruusteknologiassa, ja datasuvereniteetti on parantunut.**

Ymmärryksen hajautuminen estetään EU:ssa.

EU on alustayrityksiin kohdistetun sääntelyn myötä malliesimerkki kansalaislähtöisestä ja hyvin reguloidusta informaatioympäristöstä. Alustojen tietojen oikeellisuutta pidetään yllä sääntelyn velvoittamana. EU turvaa yhteiskunnallista luottamusta ja yhteistä tietopohjaa vahvan tunnistautumisen takana olevilla alustoilla. **Ulkomaiset toimijat velvoitetaan avaamaan algoritmiensa läpinäkyvyys**, ja niiltä edellytetään sisällön todentamista synteettisen ja orgaanisen välillä. Käyttäjille ohjataan laitteisiin sisäänajetulla generatiivisella palvelumuotoilulla vaivihkaa turvallisia tapoja toimia. Virallisia informaatioympäristöjä syytetään toisaalta sensuurista.



Politisoituminen syö teknologiayritysten valtaa.

Globaalit teknologiayritykset valitsevat geopoliittiset viiteryhmänsä toimien suurvaltakilpailun osapuolina. Niillä on intressi Kiinan tai Yhdysvaltojen vaikutuspiirien levittämiseen asiakaskuntiensa laajentamiseksi. **Politisoituminen on kuitenkin syönyt teknologiajättien luotettavuutta, ja seurauksena ne joutuvat tekemään EU:ssa sääntelyn mukaisia myönnytyksiä** ja toimimaan paikallisemmin jatkaakseen data -ja alustataloustoimintaansa ja ylläpitääkseen markkina-alueitaan. EU:ssa huolehditaan, ettei niille päädy tietoa kärkiteknologioiden greenfield-yrityksistä tai arvokkaasta, erikoistuneesta datasta.

Toimitusketjut eivät ole palanneet globaaleiksi.

Kiina-keskeiset globaalit toimitusketjut ovat säilyneet maailmantalouden keskeisimpänä väylänä, mutta **Kiinan ja Yhdysvaltojen välillä on rajattu toisen palveluita ja infrastruktuuria.** Kiinalaisen teknologian hyödyntäminen on kielletty monessa EU-maassa kriittisen infrastruktuurin ydinalueilla, mutta sen palvelut ja laitteet ovat lisääntyneet kuluttajamarkkinoilla. **EU on lisännyt yhteistyötä länsimaiden kanssa ja ylläpitänyt neutraaleja kauppasuhteita Kiinaan ja BRICS-maihin Venäjää lukuun ottamatta.** Kauppasuhteiden parantamista mm. Afrikan suurimpiin talouksiin kartoitetaan. Venäjä on uudelleenintegroitu muodollisesti maailmantalouteen Yhdysvaltojen ajamana, mutta sen suhteet suurimpaan osaan EU-maista ovat pysyneet kireinä.

Kybersääntely kiristyy.

EU on johtoasemassa teknologian ja kyberturvallisuuden sääntelyn ja standardien määrittäjänä. **EU:ssa rakennetaan strategisen autonomiapyrkimyksen tukemana demokratiaa ja yksityisyydensuojaa ylläpitävää tekoälysovellutusten ja datankäytön sääntely-ympäristöä, mihin kansainväliset teknologiayritykset joutuvat sopeutumaan.** Vahvaan tunnistautumiseen perustuva EU-pilviympäristö takaa sääntelynmukaisen tietoturvan minimitason. Länsimaissa on vallalla suuntaus, jossa suojeltavan datan arvo määrittää käytännössä turvaamisen painopisteet. Yrityksillä on kannustin tietoturvasääntelyn noudattamiselle arvokkaan ja todennetun *luomudatan* kohdalla.

Vastakkainasettelu säilyy suurvaltojen etupiirien välillä

Geopolitiikkaa ja maailmantaloutta leimaa Yhdysvaltojen kanssa tehtävien diilien aikakausi Kiinan kilpailukyvyn lähestyessä sen tasoa. Yhdysvallat on kohdannut *Dotcom 2.0-talouskriisin* teknologiayritysten ja finanssisektorin paisuttaman LLM-tekoälykuplan myötä ja sen yritysten kansainvälinen asema on heikentynyt. **Samalla se on kuitenkin onnistunut säilyttämään suhteellisen johtoasemansa kääntämällä kolmansia valtioita kahdenvälisillä sopimuksilla Kiinaa vastaan**, joka nähdään yhä useammin sponsorin sijasta velkojana. Suoranaisten geopoliittisten yhteenottojen sijaan **käynnissä on kilpailu teknologiasta, liittolaisista ja luonnonvaroista mahdollisiin konflikteihin valmistautumiseksi.** Sodan kynnyksen alittavat toimet leimaavat tasaisesti suurvaltojen ja niiden etupiirien välejä.

Intian ja Kiinan suhteiden kiristyminen on vähentänyt jälkimmäisen geopoliittista liikkumatilaa, eikä BRICS-yhteistyö ole konkretisoitunut jäsenmaiden pitäessä pintansa Kiinan talousdominanssia vastaan Venäjää lukuun ottamatta. **Venäjä on integroitunut osin takaisin globaaliin talouteen** energia- ja raaka-ainemarkkinoille. EU:n ja Venäjän välit ovat pysyneet kireinä.

Sisäisten haasteiden seurauksena autokraattisemmaksi ja arvaamattomammaksi liittolaiseksi muuttuneet **Yhdysvallat on protektionistisesta tempoilusta huolimatta ylläpitänyt sitoutumistaan mm. Nato-yhteistyöhön**. EU ja yhteistyökumppanit Commonwealth-maista, Japanista ja Etelä-Koreasta ovat turtuneet Yhdysvaltojen protektionistisiin impulsseihin, ja muodollisten liittolaistenkin toisilleen asettamat teknologiset ja taloudelliset kepit ja porkkanat ovat ylipäätään maailmanpolitiikan arkipäivää. Muut länsimaat pyrkivät vähentämään teknologisia riippuvuuksiaan Yhdysvalloista siellä, missä se on mahdollista.

Toimitusketjut eivät ole palanneet globaaleiksi

Kiina-keskeiset globaalit toimitusketjut ovat säilyneet maailmantalouden keskiössä. Kiina ja Yhdysvallat ovat rajanneet voimakkaasti toistensa yritysten palveluiden ja infrastruktuurin käyttöä. Yhdysvaltojen liittolaismailta vaaditaan yhä vahvemmin irtautumista kiinalaisesta infrastruktuurista ja palveluista. Kiinalainen teknologia onkin kielletty monessa EU-maassa infrastruktuurin ydinalueilla, mutta sen palvelut ja laitteet ovat lisääntyneet kuluttajamarkkinoilla. **EU joutuu toimimaan edelleen laajasti riippuvaisena Yhdysvaltojen teknologioista pyrkiessään samalla pitämään yksilönvapaudet ja yksityisyyden digitalisaatiokehityksen keskiössä.**

EU:n komissio on tunnistanut Yhdysvaltojen suuryritysten vähentyneen liikkumavaran myötä mahdollisuuden kriittisen datan kotiuttamiseen ja parantanut omavaraisuuttaan erityisesti suvereenien pilviratkaisujen muodossa. EU-julkipilviekosysteemissä suojellaan kansalaisten sensitiivistä dataa sekä hallinnoidaan kriittisimpiä tietojärjestelmiä omissa datakeskuksissa. Yritykset ovat muodostaneet toimialadatan kerryttämiseen perustuvia varantoja, josta sisämarkkinan ulkopuoliset yritykset maksavat käyttömaksun. EU:ssa on käytössä eID-henkilöllisyys, jonka käyttöoikeuksien hallintaa se ohjaa.

EU:n yhteismarkkina on saanut yritykset kasvuun ja datan yhteiskäytettävyys ottaa harppauksia. Kokonaisvaltaisen digitaalisen suvereniteetin tavoittelu osoittautuu kuitenkin EU:lle vaikeaksi, vaikka luottamus Yhdysvaltoihin ja sen yrityksiin on hiipunut. EU:n suvereeni pilvikapasiteetti koskettaa etupäässä sensitiivisimmän käsittelyn alustoja, joita käytetään muita tietoja sääntelyn mukaisesti käsittelevän yhdysvaltalaisen hyperskaalan rinnalla.

Kybersääntely kiristyy

EU on ylläpitänyt johtoasemaansa teknologian ja kyberturvallisuuden sääntelyn ja standardien määrittäjänä. EU pyrkii rakentamaan strategisen autonomiapyrkimyksen tukemana digi- ja kybersääntelyn ”kolmatta tietä”, eli demokratiaa ja yksityisyydensuojaa ylläpitävää tekoälysovellutusten ja datankäytön sääntely-ympäristöä, pyrkien tekemään siitä globaalisti vaikuttavan vastavoiman Kiinan ja Yhdysvaltojen järjestelmille. Reguloitu EU-pilviympäristö takaa kansalaisille sääntelynmukaisen tietoturvan ja tietosuojan minimitason.

Tiukentuneesta sääntelystä huolimatta länsimaissa on yleisesti vallalla yritysten sääntelynmukaisuuden ja riskinoton välillä tasapainoileva suuntaus, **jossa suojeltavan datan arvo määrittää käytännössä turvaamisen painopisteet.** Yrityksillä on kannustin tietoturvasääntelyn noudattamiselle erityisesti arvokkaan ja todennetun *luomudatan* kohdalla, ja sen suojauskeinoja kehitetään erityisesti mahdollisen vuotamisen johtaessa suurempaan sanktiohintalappuun. Privacy data-pörssi asettaa tiedolle hinnan alueellisissa, samanmielisissä geopoliittisissa vertaiskuplissa, ja omat variaatiot muodostuvat länsimaihin sekä Digital Belt & Road-valtioiden välille. **Hyväosaisilla on mahdollisuus saattaa yrityksiä vastuuseen ja maksaa turvallisuudestaan, mutta muiden väestöluokkien tietosuojan suhteen otetaan käytännössä enemmän riskejä.**

Sääntelyä koskeva valvonta ja tiedonvälitys toimii geopoliittisten alueiden, kuten länsimaiden ja Digital Belt and Road-maiden sisällä niiden viranomaisten välillä. Etupiirien välinen yhteistyö on vähentynyt. EU-rahoituselimet lisäävät vaikutusvaltaansa strategisen omavaraisuuden hallinnoinnissa.

Politisoituminen syö teknologiayritysten valtaa

Suuret teknologiayritykset joutuvat maailmalla vallitsevan protektionismin myötä valitsemaan pääasialliset geopoliittiset viiteryhmänsä ja markkinansa Yhdysvaltojen ja Kiinan väliltä. Niillä onkin taustaintressi suurvaltojen geopoliittisten vaikutuspiirien levittämisen auttamiseen mahdollisten asiakaskuntiensa laajentamiseksi. **Politisoituminen on kuitenkin syönyt suurien teknologiayritysten luotettavuutta, nostanut vastustusta sekä johtanut paikallisten kilpailijoiden asemien kohentumiseen**, ja seurauksena ne joutuvat tekemään EU-sääntelyn mukaisia myönnytyksiä jatkaakseen täysimääräisesti data -ja alustataloustoimintaansa alueella.

EU:ssa huolehditaan, ettei ulkomaisille suuryrityksille päädy tietoa teknologia-alan greenfield-yrityksistä tai arvokasta, erikoistunutta toimialadataa. Ne joutuvat tasapainoilemaan EU:n markkina-alueen ja kansalaisten luottamuksen ylläpidon, sekä emomaidensa poliittisten tavoitteiden välillä kallistuen kuitenkin useimmiten ensin mainittuun.

Matalaa autonomiaa ja laadukasta dataa

Ensimmäistä LLM-sovellusaaltoa ei saada voitolliseksi ja **infrastruktuurin ylirakentaminen, ratkaisujen ylimyynti ja romahtaneet tuotto-odotukset ovat saaneet rahoittajat vetämään investointejaan takaisin.** Suurimpien mallien manipulaatio-ongelmia ja hallusinointia ei ole saatu ratkaistua. AI-generoitu sisältö ja synteettinen data on lisääntynyt, mutta sitä ei voida hyödyntää rekursiivisesti mallien jatkokehitykseen. Autenttisen ja laadunvarmistetun *luomudatan* arvo on lisääntynyt. Skaala edellä rakennetut mallit ovat osoittautuneet vääräksi lähestymistavaksi luotettavaan ja autonomiseen AI-teknologiaan. Volyymiin perustuvan kehityksen osoittauduttua kannattamattomaksi suorittimien ja näytönohjaimien saatavuus on parantunut. Laskentaa siirtyy suurista pilvitoteutuksista enenevästi rajatumpiin tehtäviin ja paikalliseksi reunalaitelaskennaksi. LLM-aalto on tehnyt tilaa SLM-aallolle ja **AI on työkalu muiden joukossa, tehostaen erityisesti ohjelmointia.**

Laadukkaan koulutusdatan EU-kielimallit ovat vakiinnuttaneet paikkansa kansalaisten arkikäytössä, **mutta teknologian työllisyysvaikutukset ovat rajallisia työkalujen rajallisen autonomian myötä,** ihmisten on yhä toimittava prosessien laadunvarmistajina. Tärkeimmät sovellutusalueet ovat **suurten ja datamassojen pohjalta tehtävässä mallintamisessa ja reaaliaikaisessa analyysissä**, jota varten EU-yritykset muodostavat toimialadatapooleja.

Matalan autonomian eID-henkilöllisyyteen kytkeytyvät tekoälyagentit pystyvät hoitamaan arjen tehtäviä ja ne ovat lyöneet EU:ssa läpi rajoituksin, jotka rajaavat niiden käyttöoikeuksia ja sallivat toimijoille yksiselitteisesti niiden estämisen.

Salausalgoritmit voittavat kvanttikilpajuoksun

Sensitiivinen data on turvattu kvantinkestävillä suojauksilla. EU on pysytellyt kvantti-infrastruktuurin rakentamisessa Yhdysvaltojen ja Kiinan vauhdissa tuettuaan yritysekosysteemejä sisämarkkinassa, ja kvantinkestävää suojausta on rakennettu keskeisiin osiin kriittistä infrastruktuuria. Ensimmäisiä perinteisen kryptografian murtamiseen toimivia ratkaisuja on kehitetty, mutta salausratkaisut ovat kehittyneet purkukeinoja nopeammin, ja hurjimmat edistysaskeleet ovat enimmäkseen informaatiovaikuttamista. **EU käyttää pitkälle kehittyneitä salausratkaisuja mm. kytkeytyneen EU-yritysekosysteemin ja kansalaisten henkilötietojen suojaamiseen.** Aiemmin kerätyn, matalammin suojatun tiedon purkaminen mahdollistuu valtiotoimijoille, johtaen organisaatioissa pakon edessä hyväksyttyyn vanhan tiedon julkistumiseen ja siitä seuraaviin riskinhallintatoimiin.

Yhteydet paranevat länsimaisessa yhteistyössä

Globaalisti standardoidun 6G:n käyttöönotto on nopeaa 2030-luvulla, ja **suuri osa laitteista ja ohjelmistoista tulee EU-jäsenmaiden lisäksi Yhdysvalloista, Etelä-Koreasta tai Japanista. Nopeat laajakaistayhteydet EU:n syrjäseuduilla toteutetaan pääasiassa EU:n oman IRIS²-konstellaation voimin, ja kapasiteettia täydennetään yhdysvaltalaisten palveluntarjoajien kautta.** Teleoperaattorit, pilvipalvelualustat ja logistiikkayritykset integroivat satelliittipalveluja tarjontaansa API-pohjaisilla kumppanuuksilla EU:ssa toimiviin, osin ulkoisesti riippuvaisiin ekosysteemeihin.

LLM-hypen yhteydessä rakennettu **laskennan ylikapasiteetti valjastetaan soveltuvilta reaaliaikaisten ja realististen etäyhteyksien rakentamiseen. EU:n sisämarkkinoiden yritysten VR-todellisuudet ovat arkipäivää organisaatioissa.** Yhteiskuntien kytkeytyminen on johtanut sensoreiden ja rajapintojen monipuoliseen yhdistymiseen. **EU:ssa teollisuuden, talouden ja yhteiskunnan järjestelmiä pyörittävät, tehostavat ja valvovat digitaaliset kaksoset ovat yleistyneet.** Teknologista kokonaisuutta mutkistavat alihankintaketjut, jossa osan palvelukokonaisuuksista tuottavat EU:n ulkopuoliset toimijat, joiden ylläpitämiin osiin järjestelmistä ei ole suoraa näkyvyyttä.

Ymmärryksen hajautuminen estetään

Huoli hajautuvasta informaatioympäristöstä ja jaetun tietopohjan romahtamisesta johtaa poliittiseen ja liikehdintään sen turvaamiseksi. **EU on alustayrityksiin kohdistetun sääntelyn onnistuttua malliesimerkki keidasmaisesta, reguloidusta informaatioympäristöstä,** jonka ytimessä ylläpidetään EU-pilvessä vallitsevan vahvan tunnistautumisen kautta aukeavaa ”virallista informaatioympäristöä”, **jonka pariin kansalaisia pyritään saamaan mediakasvatuksella ja vaikuttamistyöllä.**

Alustojen tietojen oikeellisuutta pyritään pitämään yllä sääntelyn velvoittamana. Ulkomaiset toimijat velvoitetaan avaamaan algoritmiensa läpinäkyvyys, ja niiltä edellytetään sisällön todentamista synteettisen ja orgaanisen välillä. Kuratoitujen tiedon keitaiden ulkopuolella rehottavat kuitenkin lisääntyneen generatiivisen tekoälyn käytön myötä seurauksena synteettisen tiedon ja disinformaation joutomaat, joilla alustat ja valtiotoimijat pyrkivät saavuttamaan totuusmonopolin.

Edulliset suorittimet, näytönohjaimet ja laskentakapasiteetti markkinoilla ovat johtaneet suorituskykyjen saamiseen uhkatoimijoiden käyttöön, johtaen mm. deepfake-teknologioiden suorituskykyjen lisääntymiseen. **Kiina ja Digital Belt and Road-maat ja toisaalta Yhdysvallat lähimpine liittolaisineen pyrkivät rakentamaan omissa *informaatioetupiireissään* synteettisten sisällöntuottajien ja kansanryhmien tukemaa tarinaansa maailmasta laajentaakseen vaikutuspiirejään.**

EU:ssa kasvatetaan tietoturvakansalaisia

Vahvan tunnistautumisen mahdollistamat, AI-assistentteihin integroituneet EU-käyttäjät tiedostetaan riskialttiiksi yhdistelmäksi biometrisiä ja henkilötietoja, ja alustojen toiminnallisuuksia rajoitetaan vahvan tunnistautumisen ympäristöissä. **Sallittujen sovellusten ja eID-virtuaalikäyttäjään kytkettävien sekä älyllisten sensoreiden lista kapenee EU:ssa** tietoturvariskien estämiseksi. Laitteista tehdään EU-sopivia versioita. Uusimpien innovaatioiden auditoinnissa ja saamisessa sisämarkkinoille kuluu aikaa, mihin kaikki käyttäjät eivät ole tyytyväisiä. Agenttien käyttöönotto alustoilla on lisännyt tarvetta vahvempaan biometriseen tunnistautumiseen, jakaen EU-jäsenmaiden suhtautumista. Kansalaisten lisääntyviin autenttisuuden, yksityisyyden ja analogisuuden vaatimuksiin pyritään vastaamaan digitaalisella normistolla. **Halu hallita omaa dataa, valita tietoisesti teknologian ulkopuolelle jättäytyminen ja käyttää ihmisten tuottamia sisältöjä kasvaa.**

Sosiaalisen median ja tekoälyalustojen mainontaa kiristetään, ja EU:n ulkopuolisista alustoista tulee maksullisia dataliiketoiminnan rajoitusten myötä. **Käyttäjille ohjataan alustoilla generatiivisella palvelumuotoilulla turvallisia tapoja toimia.** Yhden objektiivisen totuuden muuraaminen EU:n informaatioympäristön peruskiveksi ei ole kuitenkaan helppoa. **Virallisia informaatioympäristöjä syytetään sensuurista, ja monet kokevat käyttäjiä disinformaatiolta suojelevan ”EU-todellisuuden” olevan demokraattisen sijaan autoritaarinen elämäntapa.**

Osa käyttäjistä **pyrkii kiertämään sovellusten ja laitteiden rajoituksia hankkimalla niitä vahvistamattomista lähteistä. Toimitusketjujen AI-anomaliaseurannan myötä** laittomien teknologioiden, laitteiden ja alustojen hyödyntäminen virallisen käyttötuen ulkopuolella eID-henkilöllisyyden kanssa johtaa karanteeniin ja pääsyn virallisiin palveluihin rajaamiseen, sekä pahimmassa tapauksessa vakoilu- ja disinformaatiosyytteisiin.

Pinta-ala: Demokraattisesti omavaraisempi infrastruktuuri

- EU:n keskitetty vahvan tunnistautumisen henkilöllisyysratkaisu käsittää merkittävän katalogin kansalaisten sensitiivisiä biometrisiä ja muita henkilötietoja, jota kertyy alueen EU-datakeskuksiin.
- AI-kilpailun toisessa aallossa korostuvat laadukkaat, yksityiset *luomudatalähteet*, joita on kerrytetty EU:n sisämarkkinoiden toimialakohtaisiin data-altaisiin ”kruununjalokiviksi”.
- EU:n strategisen autonomian ponnistelujen myötä energiainfrastruktuurin sähköistyminen lisännyt uusiutuvan energian potentiaalia, painottaen älyverkkoja, joihin kytkeytyy väistämättä EU:n ulkopuolelta peräisin olevia komponentteja.
- Lisääntynyt IoT- ja IIoT-kytkeytyminen kasaa reunalaitteita etenkin suurimpien kaupunkien Smart City-kokonaisuuksissa, joissa yhteiskunnan toiminnan dataa kertyy toimintoja optimoiviin datamyllyihin ja digitaalisiin kaksosiin. Kansalaisille näkyvä osa linkittyy oman AI-assistentin kautta mm. navigointiin ja liikenteenohjaukseen, johtaen parempiin palveluihin.
- EU-maiden todennettava ja validoitu tieto on keskittynyt vahvan tunnistautumisen takana avautuvaan todennetun tiedon informaatioympäristöön, joka editoi aktiivisesti kansalaisille välittyvää kuvaa maailmasta disinformaation vastatoimena. Henkilökohtaisina informaatioympäristön todentajina ja kuratoijina toimivat EU-kielimallin välityksellä toimivat AI-assistentit.
- Tarvittavien kyberosaajien määrää ei ole saatu kurottua kiinni EU:ssa etenevän ikääntymiskehityksen myötä, ja ammattilaisia on pyritty rekrytoimaan proaktiivisesti muualta haavoittuvuuspinta-alan hallitsemiseksi. Edulliset suorittimet ja erikoistuneet mallit ovat toisaalta mahdollistaneet autonomisen kyberpuolustuksen kevyitä ratkaisuja.
- Vahvan eID-tunnistautumisen vaatimus ja EU-alueella rajattu sovellusvalikoima ehkäisee kansalaisten ajautumista uhkatoimijoiden AI-avusteisesti koodaamiin, urkintaan käytettäviin kopioversioihin sovelluksista.

Uhat: Sodan kynnyksen alittavia operaatioita

- Valtiotoimijat tiedustelevat ja miinoittavat länsimaiden järjestelmiä konflikteja ennakoiden. Toiminta pidetään sodankäynnin kynnyksen alapuolella.
- EU-kielimallin ilmentyminä toimivat henkilökohtaiset AI-avustajat voidaan ohjelmoida vaikuttamaan vaivihkaa niistä arjessaan riippuvaiseksi tulleisiin kansalaisiin. EU-kielimallin assistentti/agenttisovellutusten koulutusdata on myrkyttämis- ja korruptointihyökkäysten kohteena disinformaation lisäämiseksi.
- AI-työkaluja voidaan käyttää tarkoilla rajauksilla ja tehtävänannoilla hyökkäämisessä ja puolustamisessa. Tiukentunut AI-sääntely-ympäristö turvallisuusvaatimuksineen hidastaa puolustussovellutusten käyttöönottoa ja kehitystä suhteessa hyökkääjien pidäkkeettömämpiin kyvykkyyksiin.
- Kyberrikolliset ovat kiinnostuneita eID:n biometriikkaa ja henkilötietoja kerryttäneiden EU-pilvipalveluiden datayhdistelmien hyödyntämisestä murroissa, huijauksissa ja kalastelussa. Järjestelmiin pyritään pääsemään sisään niiden parissa työskentelevien henkilöiden kautta.
- EU:n jäsenvaltioiden tietopalveluihin, kuten tilastokeskuksiin kohdennetaan hyökkäyksiä kansalaisten rekisteridatan saamiseksi haltuun ja käänteismallinnettavaksi tekoälyavusteisesti personoituja hyökkäyksiä varten.
- EU-maiden uusiutuvan energian infrastruktuuriin kohdennetaan kyberhyökkäyksiä ja sabotaasia, tarkoituksena heikentää luottamusta uusiutuviin energiamuotoihin.
- *Luomudatan* painotus AI/ML-kehityksessä tekee yritysten toimialadatasta houkuttelevaa ja arvokasta vakoiltavaa.
- Vakoilu- ja sabotaasitoimintaa kohdistetaan digitaalisten kaksosten Smart City-solmukohtiin. Risteyskohtia hyväksikäytetään murtautumisessa yksittäisiin sensoreihin ja konesaleihin, sekä manipuloimaan kaksosten AI-rajapintoja.
- Uusimpia innovaatioita ja sovelluksia toivovia kansalaisia pyritään manipuloimaan ja kytkemään eID-käyttäjäänsä laittomia laitteita ja sovellutuksia urkintatarkoituksessa.


/PIRSTALOITUMINEN/

/PIRSTALOITUMINEN 2035/

Kriisit hidastavat teknologioiden omaksumista.

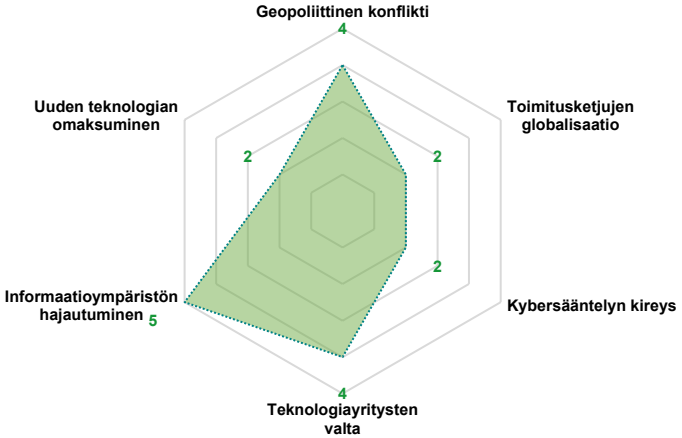
Suurien teknologiayritysten johdolla käyttöön otettujen AI-rajapintojen ja LLM-koodattujen turvattomien ja heikosti ylläpidettyjen ratkaisujen kautta on päästy laajasti käsiksi arkaluontoiseen tietoon **”AI-katastrofissa”.** Yhteiskuntien rakenteissa käyttöön otettuja AI-sovellutuksia on demokratioissa viritetty vakoiluun, disinformaatioon ja manipulaatioon, ja niiden keräämää **tietoa on onnistuttu takaisinmallintamaan yksilöihin ja organisaatioihin**. Organisaatiot joutuvat tekemään AI-työkalujen käyttöönotossa merkittäviä riskiarvioita, ja käytetyt ratkaisut ovat usein kapeita, mutta **vahinko on yksityisyyden kannalta jo tapahtunut**. Teknologiset standardit mm. 6G:ssä ovat erkaantuneet voimakkaasti. Epäluulo yhdysvaltalaista teknologiaa kohtaan hidastaa uuden teknologian käyttöönottoa ja ajaa joitain maita Kiinan leiriin **tehden EU:n infrastruktuurista tilkkutäkkimäistä.** Kvanttiturvallisista salausratkaisuista toivotaan yhteiskunnallisen luottamuksen palauttajaa, mutta EU on kehityksessä jäljessä.

Mihinkään ei voi luottaa.

Julkisen internetin käytettävyys on romahtanut kun tekoälyllä luotu synteettinen materiaali ja vuorovaikutus on vallannut elintilan, ja kehitystä on paettu suljetumpiin yhteisöihin. Älyjärjestelmistä vuodettuja tietoja on käytetty yksilöiden ja yritysten kiristämiseen, oikeustapaukset ovat lisääntyneet ja suhtautuminen datan luovuttamiseen kiristyy, vähentäen saatavilla olevaa AI-koulutusdataa. Eri palveluntarjoajien alustoilla vallitsee erilaisia maailmankuvaa muovaavia totuuspohjia. Vaatimukset askeleiden ottamiseksi taaksepäin digitaalisen saasteen täyttämästä informaatioympäristöstä ovat lisääntyneet. **Kansalaisyhteisöissä otetaan käyttöön *Nightshaden* kaltaisia sensoreiden ja älyominaisuuksien myrkyttämis- ja huijauskeinoja** yritysten ja viranomaisten algoritmeilta pakenemiseksi.

Maailma on tuuliajolla, geopoliittinen tilanne arvaamaton.

Yhdysvallat on hylännyt kansainvälisen yhteistyön foorumit ja keskittynyt ajamaan omaa välitöntä etuaan. Autoritaariset valtiot levittävät vaikutusvaltaansa **ajamalla EU:ta ja demokratioita erilleen kärjistämällä sisäisiä ja keskinäisiä ristiriitoja,** sekä taloudellisin kannustimin. Väestöt ovat jakautuneet suuryritysten teknologioiden ympärillä eläviin, sekä teknologista globalisaatiota vastustaviin ryhmittymiin. Yhteinen kannanmuodostus on vaikeutunut heikentäen EU:ta sääntelytahona.



Riippuvuudet syvenevät epäluottamuksesta huolimatta.

Suuret teknologiayritykset kamppailevat käyttäjistä, datasta, energiasta ja markkina-alueista ilman suuria esteitä. Kiinan teknologisen vaikutuspiirin kasvu nostaa esteitä länsimaisten ratkaisujen leviämiselle, ja pienentyvä markkina-alue ajaa länsimaisia yrityksiä syventämään paikkaansa demokratioiden julkishallinnoissa. Ne omaksuvat vahvemmin aseman yhteiskuntien digitalisaation laadunvalvojina ja ylläpitäjinä, saaden vastineeksi poliittistakin valtaa, kohdaten samalla joissain väestönosissa aiempaa laajempaa vastustusta ja irtautumista. **Niiden erikoistuneet alihankintaketjut** ja ekosysteemien identiteetinhallintapalvelut takaavat yhteiskuntien digitaalisen jatkuvuuden.

Toimitusketjut alueellistuvat.

Teknologian saatavuushaasteet vaikeuttavat tieto-yhteiskunnan ylläpitoa ja EU on suurien toimitusketjujen hallitsijoiden armoilla jatkuvuuden takaamiseksi. Jäsenmaat jakautuvat talous- ja turvallisuusintressiensä suhteen ja lobbauksen seurauksena yhdysvaltalaisia tai kiinalaisia ratkaisuja suosivien leireihin, ehkäisten yhtenäistä infrastruktuuripolitiikkaa. Seurauksena on **EU:n pirstaloitunut digitalisaatiokehitys,** jossa Länsi-Euroopassa tehdään hankinnat Yhdysvalloista tai muista länsimaista, tai rakennetaan omia yhteisratkaisuja. **Itä-Euroopan maissa puolestaan tehdään harppauksia Kiinan Digital Belt And Road-integroituneen teknologian ja infrastruktuurin siivittämänä. Toimitusketjujen** hallintakyvyn heikennyttyä turvattomat laitteet ja haavoittuvat tietoverkot ovat yleistyneet.

Realisoituneet uhat ovat sääntelylle liikaa.

Yhä useamman valtion julkishallinto ”romahtaa” digitaalisesti kun päätöksentekijät eivät hallitse arvaamatonta teknologista kokonaiskuvaa riskeineen ja riippuvuuksineen. Suuryritykset onnistuvat torppaamaan demokratioissa sääntelypyrkimyksiä pysytellen vain itse ymmärtämänsä teknologisen kehityksen kärjessä. **EU:n päätöksenteko on blokkiutunut sisäisesti jakolinjojen lisäännyttyä ja jäsenmaiden jakauduttua pienempiin intressiryhmiin, jähmettäen komission toimintakykyä.** Tulenarka toimintaympäristö keskittää ponnistuksia akuutteihin turvallisuuskysymyksiin ja peruskäyttäjän suojaaminen ulkoisilta uhkilta ja yritysten mielivallalta jää sivuun. Kansalaisten kyky nauttia sääntelyn takaamasta digiperusturvasta heikentyy, eivätkä EU-jäsenmaat voi enää taata sitä heikoiten toimeentuleville.

Maailma on tuuliajolla, geopoliittinen tilanne arvaamaton

Yhdysvallat on hylännyt kansainvälisen yhteistyön foorumit. Sen sotilaallisten interventioiden tuoma rasitus ja kärjistyneen talouskriisin luoma epävakaus on ajanut sitä edistämään omaa välitöntä etuaan, tehden liittolaisuudesta transaktionaalista. **Eletään moninapaisen pirstaloitumisen aikaa, jossa Kiina liittolaisineen liikkuu valtatyhjiöihin.** Maailman pelisäännöt ovat uudelleenneuvottelun tilassa. Yhdysvaltojen ja Kiinan yksipuolisesti harjoittama suvereniteettia uhkaava sanelupolitiikka on lisääntynyt, johtaen Eurooppaa ja Aasiaa koskettaviin rajattuihin alueellisiin konflikteihin ja taloudellisten aseiden käyttämiseen, heikentäen globaaleja toimitusketjuja ja teknologian saatavuutta.

Euroopassa on herätty AI-vallankumouksen jälkeen tilanteeseen, jossa **sovellutukset eivät ole lunastaneet tehokkuuslupauksiaan ilman merkittävästi lisääntyneitä turvallisuusongelmia. Pistemäisesti kehitettyjen ja harkitsemattomasti käyttöön otettujen AI-sovellutusten ja rajapintojen kautta on päästy käsiksi arkaluontoiseen tietoon,** ja seurauksena poliittista vaikutusvaltaa ja sosiaalista kontrollia on siirtynyt käyttöliittymien välityksellä ja kerätyn tiedon käänteismallintamisen myötä ulkopuolisille. Autokratiat ovat suojelleet kansalaisiaan ulkomaiselta teknologialta, mutta **demokratioissa laajalle levinneitä sovellutuksia on viritetty kehitysvaiheessa ja käytön aikana tietoisesti ja tiedostamatta moninaiseen ulkopuoliseen vakoiluun, disinformaation levittämiseen ja arvopohjan manipulaatioon.** Seurauksena ymmärrys yhteisestä totuudesta on järkkynyt, kokemus tietoturvasta ja suojasta kadonnut, ja sisäiset konfliktit kärjistyneet. *Tekoälykatastrofin* osaltaan edistämä **polarisoituminen ja heimoistuminen** on kaventanut demokratioiden toimintakykyä.

EU:ta ja demokratioita ajetaan erilleen kärjistämällä niiden sisäisiä ja keskinäisiä ristiriitoja. Väestöt ovat EU:n sisällä jakautuneet suuryritysten teknologioiden ympärillä eläviin heimoihin, sekä teknoglobalisaatiota poliittisen kentän eri puolilla omalla tavallaan vastustaviin ryhmittymiin. Yhteinen kannanmuodostus on vaikeutunut heikentäen EU:ta sääntelytahona. Sen demokraattiset instituutiot ovat muodollisesti pystyssä, mutta käytännössä jäsenmaat käyttävät niitä etunsa ajamiseksi pelaten taustalla omia pelejään.

Toimitusketjut ja EU-alueen infrastruktuuri hajautuvat

Luottamussuhteiden heikennyttyä toimitusketjut ovat alueellistuneet. Mineraalien ja teknologian saatavuushaasteet vaikeuttavat länsimaissa tietoyhteiskuntaa ylläpitävien laitteiden ja palveluiden käyttöä, ja EU on suurien toimitusketjujen hallitsijoiden armoilla toimitusvarmuuden turvaamiseksi. Jäsenmaat jakautuvat talous- ja turvallisuusintressiensä suhteen ja lobbauksen seurauksena yhdysvaltalaisia tai kiinalaisia ratkaisuja suosivien leireihin, **estäen yhtenäistä infrastruktuuripolitiikkaa.**

Yhdysvaltojen suuret teknologiayritykset markkinoivat itseään EU:ssa Kiinan ratkaisuja turvallisempana vaihtoehtona, tarjoutuen julkishallintojen strategisiksi kumppaneiksi. Seurauksena on **EU:n voimakkaasti pirstaloitunut digitalisaatiokehitys**, jossa Suomi ja länsieurooppalaiset maat tekevät hankintansa Yhdysvalloista tai muista länsimaista tai rakentavat valtioryhmiensä yhteisratkaisuja. Itä-Euroopassa puolestaan otetaan käyttöön kiinalaisia, edullisia ja kattavia kokonaisratkaisuja.

Pohjoismaat sekä läntinen ja keskinen Eurooppa ovat tiivistäneet yhteistyötään. Epäluulo yhdysvaltalaista ja kiinalaista teknologiaa kohtaan yhdistettynä omien ratkaisujen rakentamiseen hidastaa ja käyttöönottoa **tehden eritahtisen käyttöönoton myötä infrastruktuurista tilkkutäkkimäistä.** Itä-Euroopan maissa tehdään harppauksia kiinalaisen Digital Belt and Road-yhteistyössä integroituneen teknologian ja infrastruktuurin siivittämänä. Toimitusketjujen hallintakyvyn heikennyttyä **halvat ja turvattomat laitteet ja epämääräiset tietoverkot** ovat yleistyneet.

Realisoituneet uhat ovat sääntelylle liikaa

Yhä useamman valtion julkishallinto ”romahtaa” digitaalisesti kun päätöksentekijät eivät hallitse monimutkaistunutta ja arvaamatonta teknologista kokonaiskuvaa. EU:n päätöksenteko on blokkiutunut sisäisesti jakolinjojen lisäännyttyä ja jäsenmaiden jakauduttua pienempiin intressiryhmiin, jähmettäen komission toimintakykyä. Suomi hakee ensisijaista vaikuttamisen viiteryhmäänsä ja luotettavia yhteistyötahoja pohjoismaista ja Länsi-Euroopasta. **Tulenarka toimintaympäristö keskittää sääntelyponnistuksia akuuteimpiin turvallisuuskysymyksiin** ja peruskäyttäjän suojaaminen ulkoisilta uhkilta ja yritysten mielivallalta jää sivuun. **Kansalaisten kyky nauttia sääntelyn takaamasta digitaalisesta perusturvasta heikentyy moninaisten riskien seurauksena, eivätkä EU-jäsenmaat voi luotettavasti taata sitä heikoiten toimeentuleville.**

Suuret teknologiayritykset hyödyntävät tilaisuuden tarjoten julkishallinnoille keskeiset palvelut ja osaamista digitaalisen yhteiskunnan tehtävien ylläpitämiseen ja jatkuvuuden turvaamiseen, vastapalveluksena kevennetty EU-sääntelyn tulkinta. Kansalaisten datankeruun ja toimitusketjujen kokonaiskuvan näkökulmasta hyödyllisimmät funktiot korvataankin pitkälti niiden tarkasti valvomilla ratkaisuilla.

Kansainvälisen sääntelyn ulottumattomissa leviävät veroparatiisit ja vapaakauppa-alueet ovat houkuttelevia toimipaikkoja yrityksille ja kyberosaajille. Ne jäytävät kansallisvaltioiden veropohjaa ja osaajapoolia, vähentäen osaltaan julkisten kyberturvallisuuselimien toimintakykyä demokratioissa. Ne toimivat usein myös kyberrikollisuuden ja APT-toimijoiden alihankinnan vaikeasti vastuuseen saatettavina alustoina.

Riippuvuudet syvenevät epäluottamuksesta huolimatta

Suuret teknologiayritykset kohtaavat demokratioissa aiempaa laajempaa vastustusta osin itse markkinoille tuomistaan työkaluista seuranneen tekoälykatastrofin myötä. Tulenarassa ja arvaamattomassa maailmantalouden toimintaympäristössä **kuitenkin ainoastaan niiden erikoistuneet alihankintaketjut, ylläpitoresurssit ja osaaminen, sekä ekosysteemien identiteetinhallintapalvelut takaavat digitaalisten yhteiskuntien jatkuvuuden**. Ne pyrkivät hyödyntämään mainettaan ohjelmistomaailman ylläpitäjinä ja laaduntakaajina AI-lähtöisten pistemäisten, teknologista kehitysvelkaa kasvattaneiden ohjelmointi-irtiottojen yleistyttyä. Koko EU:n kattavien yhteisten sovellusvaihtoehtojen rakentaminen kohtaa poliittisia esteitä, mutta päättäväisimmät jäsenvaltiot ja ryhmät rakentavat omia ratkaisujaan.

Suuret teknologiayritykset kamppailevat käyttäjistä, datasta, energiasta ja markkina-alueista. Yhdysvaltalaiset suuryritykset ovat oppineet valtiollisen politisoitumisen riskeistä ja päätöksenteon arvaamattomuudesta ja kasvattavat profiiliaan ohi liittovaltion, pyrkien vaikuttamaan itsenäisesti markkina-alueidensa sääntelyyn ja politiikkaan luodakseen itselleen suotuisaa toimintaympäristöä demokratioissa. **Kiinalaiset suuryritykset vahvistavat valtion tuella otettaan Digital Belt and Road-maiden infrastruktuureista,** rakentaen yhteiskuntien digitalisaation tehokkaat palvelut ja toisaalta käyttäjien valvonnan mahdollistavat kokonaisratkaisut.

Kiinalaisen teknologisen vaikutuspiirin leviäminen nostaa globaalissa etelässä esteitä länsimaisten teknologiayritysten ratkaisujen leviämiselle, **pienentyvä markkina-alue ajaa länsimaisia yrityksiä syventämään osallisuuttaan julkishallinnoissa,** ja vaikeassa taloustilanteessa tehtyjen sopimusten myötä palveluntarjoajille keskittyy usein tarkoituksenmukaista enemmän käyttäjädataa ja pääsyjä, joita käytetään aktiivisesti toimittajalukkojen rakentamiseen.

Tekoälykatastrofi romahduttaa luottamuksen

Agenttiset AI-sovellutukset ovat juurtuneet harkitsematta syvälle demokraattisissa yhteiskunnissa. Korkeamman tuottavuuden motivoimat nopeat lanseeraukset ovat keskittäneet sensitiivistä dataa ulkoisten palveluntarjoajien järjestelmiin, **tarjoten organisaatioiden toiminnasta ja järjestelmistä yksityiskohtaista näkymää ulkopuolisille toimijoille**. Monipuolisten sensitiivisten henkilö- ja järjestelmätietojen kasautuminen on mahdollistanut alustojen vakoilua ja manipulaatiota valtioille ja yrityksille, mutta myös kertyneen datan käänteismallintamisen rikollisille uhkatoimijoille.

Poliittisia päätöksiä on perusteltu tekoälyn tuottamalla tiedolla, ja sitä on käytetty päätöksenteon tukemisen ohella oikeutuksena epäoikeudenmukaistenkin ratkaisujen legitimointiin. **Pimeitä käytäntöjä sisältäviä sovellutuksia on myyty julkisorganisaatioille ja niitä myrkytetään geopoliittisin tarkoitusperin.** Saastumisen myötä tiettyihin toimintoihin ei voida luottaa ja käyttöä yritetään rajoittaa, mutta **yhteiskunnat eivät paikoin kykene enää toimimaan ilman niitä, eikä hahmoteta, missä malleja on käytössä.**

Tekoälyn käyttöönoton tahti on hidastunut. Kynnys agenttisten AI-toimintojen sallimiseen on korkea ja niiltä puolustautumiselle on kysyntää. Myös uhkatahot hankkivat aktiivisesti kehittyneimpiä AI-työkaluja ja agentteja käyttöönsä. LLM-buumia seurannut kehityksen hidastuminen on johtanut **laskennan ylikapasiteettiin ja myyntiin.** Rikolliset perustavat kryptovaluuttayrityksiä hankkiakseen niiden varjolla operaatioihinsa laskentatehoa. **Uhkatoimijat ovat päässeet rakentamaan keräämällään datalla ja laskennalla edistyneitä ja erikoistuneita AI-hyökkäystyökaluja.**

Kvanttisalaus luottamuksen palauttajana

Kvanttiturvallisesta kommunikaatiosta ja salausratkaisuista pyritään kuumeisesti rakentamaan **luottamusratkaisuja järkkyneelle informaatioympäristölle.** Kvanttitutkimuksen keskeisimmät areenat ovat suuryritysten ja kansainvälisen yliopistoverkoston liitoksissa. **Yritysten kvanttiosaaminen on merkittävä kybervakoilukohde.** Suurvallat väittävät rakentaneensa purkutyökaluja, joilla on pääsy vastapuolen kaikkiin järjestelmiin, mutta todellisuudessa molemmat ovat rakentaneet keskeiset järjestelmänsä ilmatiiviiksi ja kvanttisuojatuksi. **Kaikki EU-maat eivät ole kyenneet siirtymään kvantinkestävään suojaukseen sisäisen hajaannuksen ja ulkoisten vaikuttamistoimien seurauksena. Merkittävä laitteiston uudistamisvelka ajantasaisten PQC-salausalgoritmien ajamiseksi sisään on myös vaikeuttanut kehitystä**. Riskinä kiireessä on vanhentuneiden, heikkouksia sisältävien standardien käyttäminen. Sovellutuksissa priorisoidaan kriittistä infrastruktuuria ja puolustussovellutuksia. Suurvallat keskittyvät murtamaan aiemmin kerättyä sensitiivistä tietoa selvittääkseen vaikuttamisen paikkoja.

Kytkeytyminen tapahtuu vailla yhteistä suuntaa

6G:n käyttöönotto hidastuu toimitusketjujen sakkaamisen myötä, sekä erityisesti käyttötapausten ja kysynnän laahatessa. Standardi eriytyy kahteen eri suuntaukseen Kiinan ja Yhdysvaltojen yritysten välillä. **EU-toimittajat eivät ole onnistuneet saamaan kilpailijaansa markkinoille**, ja EU kytkeytyy Yhdysvaltojen rakentamaan standardiin. Moninapainen ja hallitsematon maailma heijastuu avaruuteen avaruusteknologian ja satelliittikapasiteetin hankkijoiden moninaistuessa. Peiteyritysten kautta toimivat rikolliset hankkivat valtiotoimijoiden tuella LEO-kapasiteettia **operoidakseen muiden verkkojen ulkopuolella**.

Hajautuneet toimitusketjut ovat johtaneet EU:ssa uusimman teknologian käyttöön saamisen hidastumiseen ja ratkaisujen epätasaiseen jakautumiseen. **Palveluista riippuvaisilla toimijoilla on erilaiset näkymät siihen, missä kriittistä dataa käsitellään, ja usein vain palveluntarjoajan sana takaamassa asiantilaa. Omien ratkaisujen rakentaminen on yhtenäisen EU-politiikan puuttuessa mahdollista lähinnä suurimmille organisaatioille ja hallinnoille.** Muille paras toimintatapa jatkuvuuden kannalta on hyödyntää mahdollisimman laajasti yhden suuren palveluntarjoajan yhteensopivia järjestelmiä, mikä johtaa EU-tasolla yhteentoimivuushaasteisiin; järjestelmät keskustelevat huonosti keskenään ja tietojen siirrettävyyteen on vendor lock-esteitä.

Synteettisyyden vallitessa mihinkään ei voi luottaa

Avoimen internetin tiedot syöneiden, rekursiivisesti itseään ja synteettistä ulosantiaan kasvattaneiden generatiivisten tekoälymallien toiminta on osoittautunut **itseään vahvistavaksi kierteeksi, ja julkisesti selattavan internetin käytettävyys on romahtanut synteettisen vuorovaikutuksen vallattua elintilan**. Kehitys rikkoo tiedonvälityksen alustojen luotettavuuden hajauttaen kansalaisten todellisuudet entistä erillisempiin, moderoituihin kupliin. **Eri palveluntarjoajien tunnistautumisella käytettävillä alustoilla vallitsee erilaisia käyttäjien maailmankuvaa muovaavia totuuspohjia**, ja mainostajatahot, synteettiset agentit ja poliittiset informaatio-operaattorit pyrkivät aktiivisesti vaikuttamaan niillä käyttäjiin. Puolueettomina faktantarkistajina myydyt henkilökohtaiset AI-assistentit integroituvat mediakanaviin analysoimaan syötteitä.

Vaatimukset askeleiden ottamiseksi taaksepäin digitaalisen saasteen täyttämästä digitaalisista informaatioympäristöstä ovat lisääntyneet Suomessa. Moni on pudonnut tai valinnut pudota yhteiskunnallisen eriarvoistumisen rinnalla etenevän digitalisaation kyydistä paitsioon. Osa aloittaa digitaalisen elämän paaston, moni tyytyy yksinkertaiseen peruspalveluelämään. Tietoverkkojen ”luomukäyttö” erillisverkkoineen, AI-agenteilta suojattuine rajapintoineen ja paikallisratkaisuineen on suosiossa harrastajien parissa, ja parhaita käytäntöjä levitetään yhteisöissä. **Julkishallinto kasaa rivejään muuratakseen luottamuksen peruskivet paikalleen ja tavoittaakseen ”menetetyt” kansalaiset.**

Darkwebin puolella ulkoasultaan siistiytyneet ja aiempaa helppokäyttöisemmät alustat ovat saaneet osakseen uutta suosiota **toisinajattelijoiden pakopaikkana julkisesta internetistä**. Ylläpitäjät ovat tuntemattomia, ja alustat usein moderoimattomia.

Järkkynyt tietoturvakokemus jakaa irtautujiin ja uskoviin

Hallitsematon maailma järkyttää tietoturvakokemusta. *Henkilökohtaista datavelkaa* 2020-luvun ajan kerryttäneiden kansalaisten yksityistietoja on päätynyt erilaisten rajapintojen kautta laajasti vääriin käsiin ja yhdistelemällä sitä personoitujen huijaus- ja kalasteluviestien kohdentaminen on mahdollistunut koskettamaan myös kokonaan sosiaalisen median ulkopuolelle jättäytyneitä käyttäjiä. **Oman lukunsa muodostavat monipuolisten henkilökohtaisten tekoälyassistenttien kanssa 24/7 aikaansa viettäneet biometrisiä tietoja ja tarkkaa käyttäytymisdataa luovuttaneet käyttäjät**, joista voidaan simuloida hyökkääjien toimesta jo täydellisiä, elävältä vaikuttavia ja halutulla tavalla vuorovaikuttavia valeavatareja esimerkiksi kiristystarkoituksessa.

Yhteiskunnallinen totuuspohja on järkkynyt ja kansalaiset ovat epäileviä datansa luovuttamisesta julkishallinnon käyttöön. Synteettisen sisällön täyttämä julkinen internet ei tarjoa vastauksia vuorovaikutuksen ollessa rikollisten agenttien ja bottien sävyttämää. Älyjärjestelmistä vuodettuja henkilö- ja organisaatiokohtaisia tietoja ja näiden pohjalta laadittuja synteettisiä sisältöjä on käytetty laajasti yksilöiden ja yritysten kiristämiseen, oikeustapaukset ovat lisääntyneet ja suhtautuminen datan luovuttamiseen kiristyy valveutuneilla kansalaisilla. **Yhteisöissä otetaan käyttöön *Nightshaden* ja *tar pitien* kaltaisia sensoreiden ja älyominaisuuksien myrkyttämis- ja huijauskeinoja yritysten ja viranomaisten algoritmeilta pakenemiseksi.** Käytetystä kielestä ja edelleen nopeasti kehittyvästä meemikulttuurista on tullut aiempaakin vahvemmin algoritmeja pakoilevien irtautujien tunnistautumiskeino synteettisen sisällön suotimisessa julkisen internetin *pimeässä metsässä*.

Eettisestä ja läpinäkyvästä datankäsittelystä on tulossa kilpailuetu, mutta muutos on hidasta ja luottamuksen rakentaminen vaikeaa. Dilemmaksi nousee digiyhteiskunnasta irtautuneiden **uudelleenintegrointi yhteiskuntaan sallien digitaalisten järjestelmien ulkopuolelle jättäytyminen.**

Pinta-ala: Järjestelmien tilkkutäkki

- Suuret palveluntarjoajat ovat tarkkoja pilviinsä kytkeytyvistä toimijoista, kun IT- ja OT-haavoittuvuuksia kartoittaneet AI-agentit ovat porautuneet toimitusketjujen läpi. Maksukykyiset käyttäjät ja yritykset joutuvat käymään läpi ”detoxin” kun omat AI-avusteisesti koodatut järjestelmät ovat osoittautuneet usein turvattomiksi, joutuen uusimaan digitaalisen identiteettinsä ja järjestelmänsä kytkeytyäkseen niiden laadunvalvottuihin ekosysteemeihin.
- Käyttäjien tietoa sijaitsee hajanaisemmissa ympäristössä ja tuntemattomissa sijainneissa vanhentuneiden ja haavoittuvien IoT -ja reunalaitteiden käsittelemänä. Paikallisemmat toteutukset on nostettu pöydälle, mitä on vaikeaa perustella liiketalousnäkökulmasta. Suomalaiset keskittyvät panostamaan etupäässä verkkosegmentointiin.
- Järjestelmiensä integriteetin suhteen varovaiset palveluntarjoajat tarjoavat turvallisia kokonaisratkaisuja korkeamman maturiteettitason varakkaammille toimijoille ja pk-yritykset jäävät laadukkaan tietoturvan osalta omilleen.
- Kansalaisilla on käytössä laajasti pimeitä käytäntöjä käsittäviä sovellutuksia, jotka voivat olla näennäisominaisuuksilla peiteltyjä datankerääjiä, uutisvirtojen faktantarkistusbotteja myöten. Yhteisöjen luotettuja paikallisverkkoja suojellaan agentteja torjuvilla ja harhauttavilla menetelmillä.
- Internetiin ja Darkwebiin on syntynyt lisää yksityisiä digitaalisia ekosysteemejä, jotka yhdessä vapaakauppa-alueiden kanssa mahdollistavat ”virtuaalivaltiot”, joissa rikollista kryptorahaa pestään legitiimiksi naamioitujen instituutioiden välityksellä. Turvasatamien valvontaan ei löydy yhteisrintamaa.
- AI-järjestelmissä ilmenneet turvallisuusongelmat ovat vähentäneet luottamusta autonomisiin kyberpuolustussovellutuksiin samalla, kun hyökkääjien rakentamat kyvykkyydet erikoistuneilla AI-hyökkäystyökaluilla menevät menojaan.
- Jatkuvuudenhallinnasta on tullut kompleksisempaa tuntemattomien solmukohtien myötä, mutta pirstaloituminen vaikeuttaa myös pahantahtoista toimintaa; erilaisiin järjestelmiin ja standardeihin perustuvien, vanhentuneidenkin teknisten kuvausten hyväksikäyttö on työlästä, eikä joka yksityiskohdasta löydy koulutusdataa AI-avusteisellekaan hyökkääjälle.

Uhat: Pirstaloituminen luo arvaamattomuutta

- Uusista virtuaalivaltioista ja sääntelyltään romahtaneiden maiden alueilta käsin operoivat, valtioiden tukemat ammattirikolliset ovat hankkineet ennennäkemättömällä tasolla laskentakapasiteettia ja hyödyntävät tehokkaita AI-työkaluja hyökkäyksiin, analyysiin ja tiedon yhdistelyyn.
- Valtiotoimijat ja rikolliset vaikuttavat satelliittikonstellaatioihin kyberhyökkäyksin, ja satelliittitoimintojen häiriöt ja katkot lisääntyvät. Matkapuhelinverkot, sähkövoimaverkkojen hallinta ja liikennejärjestelmät kärsivät synkronointihäiriöistä ja aika -ja paikkatiedon väärentymisestä.
- Seuranhakupalveluiden vuorovaikutustietojen, internet-selausdatan, LLM-käyttödatan, terveyssovellutusten biometriikan ja pankkitietojen yhdisteleminen ja laajat vuodot mahdollistavat rikollisille lähes rajattomat mahdollisuudet vahvasti profiloitujen, tunnepohjaistenkin deepfake-huijausten toteuttamiseen.
- Uhkatoimijat valjastavat koodiagentteja laatimaan luotetuista sovellutuksista ja alustoista hetkessä aidoilta näyttäviä kopioita, joihin houkutellaan pahaa-aavistamattomia käyttäjiä.
- Euroopan 2020-luvun Venäjän hyökkäyssodassa teroitetut molempien osapuolien huippukyberkyvykkyydet ovat kaupan maailmanmarkkinoilla.
- *AI-nollapäivähaavoittuvuuksia* esiintyy, kun mallien muistiin, oppimisdataan tai kontekstiin on piilotettu ja piilotetaan tietyin ehdoin laukeavia haavoittuvuuksia esimerkiksi AI-sovelluksen pitkäaikaisen muistin manipulaatiolla.
- Valtiotoimijoiden ja virtuaalivaltioiden rikollisryhmittymien legitiimiksi naamioidut työalustat tarjoavat ammattilaisille lisätienestejä. Niillä pyritään rekrytoimaan paikallisia sisäpiiriläisiä deepfakeihin varautuneista IT-alan yrityksistä.
- Tehoton pakotevalvonta EU:n pirstaleisessa sääntely-ympäristössä on johtanut rikollisten hyödyntämien lunnastroijalaisten kasvuun, kun lunnaiden maksamiselle ei ole kauppapoliittisia esteitä ja yritykset pyrkivät ensisijaisesti pitämään kiinni maineestaan. Kärsijänä ovat erityisesti pk-yritykset.
- Tekoälykatastrofin jälkimainingeissa yhä useampi järjestelmä on suojattu AI-agentteja jarruttavilla ja juoksuttavilla *”tar pit”* -vastamenetelmillä, mutta menetelmiä kehitetään myös rikollisten toimesta ansana organisaatioiden hyödyntämien scrape-työkalujen ja AI-agenttien toiminnan korruptointiin.


/KAKSI VALTAKUNTAA/

/KAKSI VALTAKUNTAA 2035/

Teknologia ottaa harppauksia puolustuksessa.

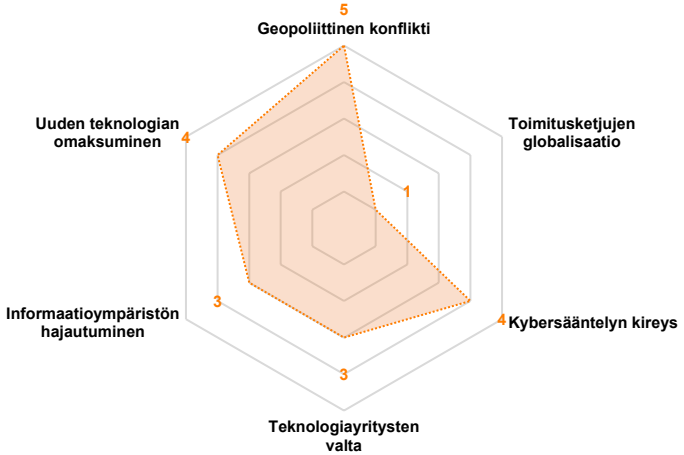
Kyberturvallisuuden autonomisista AI-sovellutuksista on tullut suurvaltojen kilpavarustelussa kriittinen osa yhteiskuntien turvallisuusarkkitehtuureja, kun **autonominen hyökkääminen on lyhentänyt merkittävästi puolustajien vasteaikaa, synnyttäen jatkuvan hyökkäävien ja puolustavien koodiagenttien kilpajuoksun. Huoltovarmuuskriittiset toiminnot** ruokahuollosta vesi-infraan **ovatkin siirtyneet tekoälyjärjestelmien hallintaan**. Ihmiset pyritään kuitenkin yhä pitämään turvallisuusympäristön kiristyessä mukana päätöksenteossa. 6G ja satelliittilaajakaistat ovat tehneet yhteyksistä geopoliittisten blokkien sisällä lähes viiveettömiä ja suurikapasiteettisia. **Kvanttiteknologiaa kehitetään suurvaltojen AI-ratkaisujen tasapelin myötä kohti sotilassovellutuksia.** Kvanttiylivoiman uhka on saanut kvanttiturvallisten algoritmien kehityksen kärkihankkeeksi, ja kriittisimmät tietovarannot on onnistuttu suojaamaan niillä molemmissa blokeissa.

Ulkopuolista informaatiovaikuttamista suitsitaan.

Tiedonvälityskanavat ja alustat ovat blokeissa ideologisen kontrollin alla. Internet säilyttää näennäisen vapauden ollen käytännössä ohjattu, suodatettu, alueellinen todellisuus. Informaatioympäristön turvaamisessa ja sitä vastaan hyökkäämisessä hyödynnetään aktiivisesti synteettistä mediaa ja deepfake-teknologioita. **Alustojen valtiollinen hallinta lisääntyy, ja käytössä on viranomaisten suodatus-, priorisointi-, ja muokkaustoimia.** Ulkoisten disinformaation levittäjien sensuuri ulottuu myös sisäisiin toisinajattelijoihin. **EU:n rooli on tietosuojan suhteen epäselvä suhteessa alustojen ylläpitäjiin, mutta tämä hyväksytään tarpeellisena uhrauksena ulkoisen ja sisäisen turvallisuuden ylläpitämiseksi.**

Geopoliittinen vastakkainasettelu on kuilun partaalla.

Yhdysvaltojen johtama länsimaiden blokki kohtaa Kiinan ja sen liittolaisten haasteen maailmanjärjestykselle. Länsimaiden yhteisrintamaa pyritään horjuttamaan testaamalla Nato-maita Euroopassa. Niiden kriittisestä infrastruktuurista etsitään aukkoja ja Naton väliintuloon suhtaudutaan laskelmoivasti. **EU:ssa on vastattu nouseviin uhkiin rakentamalla digitaalisia puolustuslinjoja yhteistyössä Yhdysvaltojen kanssa, lähes täysin riippuvaisena sen teknologioista ja Natosta.**



Teknologiajätit komennetaan riviin.

Teknologiajätit **osallistuvat julkishallinnoilleen alisteisina** suurvaltojen geopoliittisiin strategioihin mm. datan hallinnan, tekoälykehityksen ja turvallisuusinfrastruktuurin osalta. Teknologiajättien geopoliittinen hyöty on kasvanut ja ne vaikuttavat hallintoihin laajentuakseen. Puolustushallinnoilla on suurissa Nato-maissa **edustukset teknologiayritysten sisällä**. Niiden **alustat toimivat tiedustelun välineinä ja kohteina**. Teknologiajätit tukevat blokkiensa vaikutusvallan kasvattamista aktiivisesti muun muassa takaporttien ja vakoiluteknologioiden avulla, toivoen vastineeksi turvattua pääsyä kriittisiin tuotannontekijöihin. **Yhdysvaltalaiset puolustusalan analytiikkayritykset ovat integroituneet EU-maiden hallintoihin.**

Etupiirit eristävät toimitusketjunsa.

Yhdysvallat pyrkii rakentamaan riippumattomia teknologisia toimitusketjuja jatkaakseen edistyksellistä sirutuotantoa, kohdaten sijaiskonflikteja Afrikassa, Etelä-Amerikassa ja Kaukasuksella. **Kauppapoliittisesti eriytyneet tavaravirrat, demografiset haasteet ja konfliktien aiheuttamat toimitushäiriöt ovat heikentäneet länsimaiden kilpailukykyä** ja Kiinan teknologinen ylivalta tekoälyn, automaation ja datainfrastruktuurin saralla on asettanut ne puolustuskannalle. Globaali digitaalinen infrastruktuuri on jakautunut kahtia. **EU:n pyrkimykset suvereniteettiin ovat jääneet ponnettomiksi** ja yhdysvaltalaisten hyperskaalaajien infrastruktuuri hallitsee kriittisissä tietojärjestelmissä. **Niiden varaan ja valvontaan rakennetaan myös EU-alueen pilviympäristöt.**

Sääntely kiristyy turvallisuuden perässä.

Blokkien välinen teknologinen yhteensopivuus ja standardit ovat heikentyneet, ja perusinfrastruktuuri perustuu geopoliittiseen blokkiin sidottuihin järjestelmiin. Yhdysvallat vaatii digitaalisen infrastruktuurin yrityksilleen mahdollisimman vapaata toiminnan ja valvonnan alaa EU:ssa perustellen tätä niiden asemalla *lännen kriittisenä infrastruktuurina.* EU-sääntelyn turvallisuuspainotus lisääntyy, mutta valuu omista käsistä, kun **Yhdysvaltojen edustajat koordinoivat viranomaisten kanssa digitaalisia rakenteita.** Valvonnan lisäännyttyä oikeus tietosuojaan on murroksessa. Suurille palveluntarjoajille on ulotettu valvontatehtäviä mm. AI-kasvojentunnistuksessa.

Geopoliittinen vastakkainasettelu on kuilun partaalla

Yhdysvaltojen johtama länsiblokki yrittää estää Kiinan ja sen liittolaisten edustaman vaihtoehtoisen teknologisen järjestyksen vaikutusvallan leviämisen maailmankaupassa, globaalissa standardoinnissa ja alueellisesti. Kiina käyttää taloudellista ja poliittista keskeisyyttään ottaakseen paikkansa yhteisten instituutioiden ja **uusien pelisääntöjen takaajana.**

Nato-maita testataan Euroopassa ”erikoisoperaatioilla”, jotka käsittävät kyber- ja hybridioperaatioita, informaatiovaikuttamista ja energia-aseen käyttöä länsimaiden rintaman horjuttamiseksi. Heikkoja kohtia etsitään kriittisestä infrastruktuurista ja Naton väliintuloon suhtaudutaan laskelmoivasti.

Demokratialtaan taantunut Yhdysvallat on pyrkinyt laajentamaan vaikutusvaltaansa voimakeinoin läntisellä pallonpuoliskolla, sekä lisäämään tiedustelua kaikkialla maailmassa. Omien konfliktiensa ja sisäisten haasteiden parissa painiva USA pyrkii rakentamaan Kiinasta riippumattomia toimitusketjuja tukeakseen puolustusteollisuutta, sirutuotantoa ja teknologisia kärkialoja. Se kohtaa kuitenkin sijaiskonflikteihin Etelä-Amerikassa, Afrikassa ja Kaukasuksella. EU:ssa on vastattu geopoliittiseen kamppailuun rakentamalla digitaalisia puolustuslinjoja yhteistyössä Yhdysvaltojen ja Naton kanssa. EU on täysin riippuvainen näiden tiedustelutiedosta ja Yhdysvaltojen yritysten tarjoamista järjestelmistä, ja menettänyt suvereniteettiaan vastineeksi turvallisuudestaan.

Etupiirit eristävät toimitusketjunsa

Geopoliittisesti eriytyneet tavaravirrat, demografiset haasteet ja konfliktien aiheuttamat toimitushäiriöt ovat heikentäneet länsimaiden kilpailukykyä suhteessa Kiinan omavaraisempaan autoritaariseen blokkiin ja globaali infrastruktuuri on jakautunut kahtia. Sirutuotanto on jakautunut uusiin uomiin Itä-Aasian sirutuotantokapasiteetin häiriinnyttyä, heikentäen erityisesti länsimaiden AI-kilpailukykyä. Kiinan teknologinen ylivalta tekoälyn, automaation ja datainfrastruktuurin saralla on asettanut tuottavuudessa takamatkalla olevat länsimaat puolustuskannalle suojelemaan innovaatiopotentiaaliaan samalla, kun **Kiinan määrältään lisääntyneissä yhteistyövaltioissa otetaan vauhdilla käyttöön edullisia ja pinossa helposti skaalautuvia teknologioita, mm. tekoälyvalvonnan välineitä.**

EU:n pyrkimykset digitaaliseen suvereniteettiin ovat jääneet ponnettomiksi, sillä länsimaiden taloudellinen liikkumatila on heikentynyt. **Yhdysvaltalaisten hyperskaalayritysten infrastruktuuri on vahvasti hallitsevaa kriittisissä tietojärjestelmissä. Niiden puolustuksen varaan rakennetaan myös EU-alueen pilviympäristöt** yhteistyön ehtona ollessa ehdoton pysyminen irti kiinalaisista ratkaisuista ja teknologiasta. **Blokkien välinen teknologinen yhteensopivuus ja standardit ovat heikentyneet,** ja jopa perusinfrastruktuuri – kuten satelliittiverkot ja 6G-tiedonsiirto – perustuu blokkiin sidottuihin järjestelmiin.

Sääntely kiristyy turvallisuuden perässä

Kiinasta on tullut merkittävien teknologisten harppauksien myötä johtava uuden teknologian standardien asettaja. Yhdysvallat on vaatinut suurille palveluntarjoajilleen suotuisaa sääntelyä ja kohtelua vastineeksi EU:n digi-infran turvaamisesta autoritaarista blokkia vastaan. Sen edustajat koordinoivat EU-viranomaisten kanssa digitaalisten rakenteiden hallintaa ylläpitääkseen strategista kokonaiskuvaa. Hyperskaalaajat ovat kehittäneet tehokkaita, autonomisia AI-sovellutuksia, joiden pysyminen turvallisina geopoliittisesti kireässä tilanteessa edellyttää kriittisten sovellutusten varmennettuja huoltotoimenpiteitä ja ylläpitoa, sekä yleisesti lisättyä digitaalisen infrastruktuurin valvontaa. Vaatimukset toiminnan jäljitettävyydelle ovat kiristyneet, ja suurille palveluntarjoajille on ulotettu valvontaa niin sallittujen sovellutusten käytössä ja kehityksessä kuin kasvojentunnistuksessakin.

Valvonnan lisäännyttyä yksilöiden ja yritysten toiminta on entistä läpinäkyvämpää julkisorganisaatioille ja tiedustelupalveluiden tarkkailulle. GDPR on käytännössä peruttu EU:ssa ja tietosuojavaltuutetun rooli on kaventunut merkittävästi. Tiedusteluviranomaisten AI-sovellutukset analysoivat toimintaa poikkeamien löytämiseksi parantaen kansallista turvallisuutta, ollen toisaalta törmäyskurssilla yksityisyyden ja oikeusturvan kanssa johtaessaan toisinaan virheellisiin tuomioihin. Oikeus tietosuojaan on murroksessa, ja yksilön tietoturvaoikeuksien tulkinnat vaihtelevat valtiosta riippuen.

Kansainvälinen datan sääntely on sirpaleista ja suuryritysten sääntelyn taso vaihtelee globaalisti ja blokkien välillä. **Sääntelyviranomaisten merkitys kasvaa, mutta käytännön toimeenpanossa on kitkaa ja vahvan lobbauksen vaikutuksia.** EU:n kyberturvallisuusrooli vahvistuu NIS2-direktiivin/kyberturvallisuuslain tuodessa valtaa ja koordinaatiovastuuta EU-instituutioille. **Digitaaliselle infrastruktuurille perustetaan omat turvaviranomaiset.**

Teknologiajätit komennetaan riviin

Teknologiajätit joutuvat toimimaan entistä selvemmin osana suurvaltapolitiikkaa, asettuen joko Yhdysvaltojen tai Kiinan vaikutuspiiriin. Ne osallistuvat aktiivisesti geopoliittisiin strategioihin – esimerkiksi datan hallinnan, tekoälyn kehityksen ja turvallisuusinfrastruktuurin osalta. Puolustushallinnoilla on suurissa Nato-maissa pysyvät edustukset suurten teknologiayritysten sisällä. **Yrityksiä hyödynnetään valtiollisen vaikutusvallan levittämisessä, ja niiden alustat toimivat sekä tiedustelun välineinä että kohteina.** Yhdysvaltalaiset puolustusalan analytiikkayritykset ovat integroituneet EU-maiden puolustushallintoihin AI-kyvykkyyksiensä myötä. Teknologiajättien geopoliittinen hyöty on kasvanut ja ne **vaikuttavat hallituksiin laajentaakseen ja syventääkseen markkina-asemiaan.**

Teknologiajätit tukevat omien blokkiensa vaikutusvallan kasvattamista aktiivisesti muun muassa takaporttien ja tarjottujen vakoiluteknologioiden avulla, toivoen vastineeksi turvattua pääsyä kriittisiin tuotannontekijöihin kuten mineraaleihin. Yhdysvaltalaiset suuryritykset pyrkivät levittämään länsimaiden vaikutuspiiriä rakentamalla toimitusketjuja ja digitaalista infrastruktuuria blokkien väleillä tasapainoileviin myötämielisiin maihin, hankkien tarpeen tullen vipuvartta avainteknologioiden vientikieltojen, poliittisen vaikuttamisen ja rajatun sotilaallisen voimankäytön tukemisen muodossa.

EU:n tiukka sääntely ei ole avannut suuryritysten kabinettien ovia, ja riippuvuudet kostautuvat. Geopoliittinen tilanne estää vapaata innovaatiota ja investointien hajautumista, kasaten osaamista yhdysvaltalaisiin suuryrityksiin, joille maa **vaatii mahdollisimman vapaata toiminnan alaa** perustellen tätä niiden asemalla *vapaan lännen kriittisenä infrastruktuurina.*

Autonominen hyökkääminen ja puolustus lisääntyy

Tekoälystä on tullut teknologisessa kilpavarustelussa kriittinen osa yhteiskuntien turvallisuusarkkitehtuuria, kun **valtiotoimijoiden ja rikollisverkostojen autonominen hyökkääminen on lyhentänyt puolustajien vasteaikaa, synnyttäen jatkuvan algoritmisen kilpajuoksun.** Autonomisia AI-malleja rakennetaan erikoistuneilla dataseteillä hyökkäystarkoituksiin, ja AI-järjestelmät valvovat infrastruktuureja ja palveluja reaaliaikaisesti, edellyttäen suurien palveluntarjoajien agenteille oikeuksia EU:n kriittisissä järjestelmissä. **Kiinalaiset ja yhdysvaltalaiset ratkaisut ovat arvoketjujen uudelleenjärjestäytymisen ja teknologisten harppauksien myötä tasaväkisiä.**

Sekä yksityisissä että julkisissa organisaatioissa AI-agentit hoitavat data-analyysiä, riskienhallintaa ja päätöksenteon tukemista. Virtuaalisten puolustusjärjestelmien reaaliaikaisina mallintajina toimivat *kyberkaksoset,* joiden simuloinnilla toteutetaan ennakoivaa analytiikkaa tietovuotojen ehkäisemiseksi ja tilkitsemiseksi. Tiedon hajautus ja pääkäyttäjien sekä pääsyn rajaaminen ovat edelleen keskeisiä mukautumismekanismeja.

Luonnollisen kielen tekoälysovellutusten käyttö on arkipäiväistynyt ohjelmoinnissa, jonka seurauksena hallinta aiheuttaa ongelmia. Suurimmat organisaatiot (esim. puolustushallinnot), ylläpitävät AI-agenttien ekosysteemeissä **moraalista, ideologista ja juridista ohjelmointia,** jota noudattamalla agentteja kalibroidaan toimimaan läpinäkyvästi viranomaisten suuntaan, ja toisaalta niitä rokotetaan ulkopuolista vaikuttamista ja ohjelmointipyrkimyksiä vastaan.

Kvanttikilpajuoksu on seuraava strateginen kärki

Kvanttiteknologia on siirtynyt kokeiluasteelta strategiseksi resurssiksi, jota kehitetään suurvaltojen tekoälyratkaisujen tasapelin myötä kohti sotilaallisia sovellutuksia. Kvanttiylivoiman uhka on saanut kvanttiturvallisten algoritmien kehityksen lännessä puolustuksen kärkihankkeeksi, ja kriittisimmät tietovarannot on suojattu kryptografiaa voimakkaammilla salausalgoritmeilla. Epäluottamusta esiintyy blokkien sisällä, kun esiin on tullut esimerkkitapauksia läpimurtojen sotilaallisesta ja tiedustelukäytöstä jopa omien liittolaisten tietojen urkinnassa.

Kytkeytynyt puolustusinfra nostaa uusia riskejä

Maailma on siirtynyt aikakauteen, jossa 6G, ohjelmisto-ohjatut verkot ja satelliittilaajakaistat ovat tehneet yhteyksistä standardeiltaan eriytyneiden geopoliittisten blokkien sisällä lähes viiveettömiä ja suurikapasiteettisia. **Tieto ei kuitenkaan liiku enää vapaasti Yhdysvaltojen, Kiinan ja EU:n teknologiarakenteiden eriytymisen myötä.** EU:n IRIS²-satelliittikapasiteettia täydennetään puolustustarkoituksessa yhdysvaltalaisten palveluntarjoajien satelliiteilla, joihin **rakennetaan aktiivisesti sisään kaksikäyttöteknologiaa alueen sisäisen ja ulkoisen valvonnan tehostamiseksi.** EU:n satelliittitoiminnot ovat riippuvaisia yhdysvaltalaisten yritysten toiminnasta.

Yhteiskunnan digiriippuvuus on kasvanut ja huoltovarmuuskriittiset toiminnot ovat siirtyneet yhä vahvemmin tekoälyjärjestelmien hallintaan vastauksena autonomisen hyökkäämisen lyhentämälle vasteajalle Laskentaintensiivisen, tekoälyavusteisen digitaalisen puolustusinfrastruktuurin ja sitä ylläpitävien energiaintensiivisten datakeskusten rakentamisen myötä **energiajärjestelmä on yhteiskunnan kriittisin solmukohta.**

Lisääntyvät verkon reunalaitteet ovat kriittinen ja kasvava ongelmakohta, kun hyökkäys niiden sensitiivistä tietoa yhteiskunnan haavoittuvuuspinta-alasta käsittelevää dataa kohtaan on jatkuvaa. **Alusta-agnostisia ratkaisuja käytetään lisäämään joustavuutta ja vähentämään lukkiutumista tiettyihin kriittisiin järjestelmiin,** ja niitä viritetään länsimaissa palveluntarjoajien välillä tehtävään joustavaan tiedon ja toimintojen siirtämiseen. **Satelliittiyhteyksistä on tullut keskeinen uhkavektori, sillä ne toimivat paikkaavana kapasiteettina sabotaasin myötä ilmenevissä fyysisten yhteyksien häiriötilanteissa.**

Ulkopuolista informaatiovaikuttamista suitsitaan voimalla

Digitaaliset tiedonvälityskanavat ja alustat ovat vahvasti suurvaltablokkien ideologisen kontrollin alla, eikä Internet ole enää käyttäjälle aidosti globaali. **Kansalaisten kokema Internet säilyttää näennäisen vapauden**, mutta on käytännössä tarkasti ohjattu, **suodatettu todellisuus.** Tekoälyavustajat kirjoittavat geopoliittisissa blokeissa hiljalleen historiaa uusiksi, ja ideologiaa kyseenalaistavaa tietoa katoaa.

Sekä informaatioympäristön turvaamisessa että sitä vastaan hyökkäämisessä hyödynnetään tekoälyä, synteettistä mediaa ja deepfake-teknologioita. Geopoliittisia propaganda-aaltoja vastaan puolustaudutaan **massiivisen käyttäjädatan ja personointi-tiedon alustoilla AI-avustajien aktiivisella sensuurilla. Mikrokohdennuksen avulla levitetään länsimaista identiteettiä ylläpitävää maailmankuvaa ja sisältöä.**

Informaatioympäristöjen valtiollinen hallinta lisääntyy, ja käytössä on viranomaisten suodatus-, priorisointi-, ja muokkaustoimia. Koulutuksessa panostetaan informaatiolukutaidon opetukseen. Yrityksiltä edellytetään parempaa varautumista ja tiedon suojaamista myös informaatioulottuvuudessa. Harhaanjohtavat yhteisöt ja vaikuttamisverkostot tunnistetaan, ja niiden näkyvyyttä rajoitetaan aktiivisesti. **Ulkoisten disinformaation levittäjien sensuuri ulottuu sisäisiin toisinajattelijoihin, ja totuus hämärtyy usein kansallisen turvallisuuden nimissä.**

EU:n rooli ja vaikuttavuus informaatioympäristön hallinnassa on epäselvää suhteessa alustojen ylläpitäjiin, kun kaikki tieto kulkee Yhdysvaltojen tiedustelulle suuryritysten ja turvallisuusalan erikoistuneiden analytiikkayritysten välityksellä. Tämä hyväksytään tarpeellisena uhrauksena EU:n ulkoisen ja sisäisen turvallisuuden ylläpitämiseksi.

Valvonta kasvaa, vastarinta lisääntyy

Irtautuminen Kiinan toimitusketjuista on nostanut kuluttajahintoja merkittävästi länsimaissa. Samalla puolustusmenot vaativat veronsa, kansallinen koheesio heikkenee EU-maissa yhteiskunnallisen eriarvoistumisen myötä ja kansalaisten digitaalista arkea ohjataan yhä enemmän turvallisuuslähtöisesti. Hyväksyttyjen sovellusten ja laitteiden listaa on rajattu, ja länsimaissa sallitaan vain EU-validoituja, yhdysvaltalaisia ratkaisuja. **Käyttöliittymien toiminnallisuuksia rajoitetaan väärinkäytösten estämiseksi**, ja henkilökohtaiset tekoälyjärjestelmät valvovat käyttäjien toimintaa poikkeamien havaitsemiseksi. Ihokosketuspinnan tunnistus (esim. älytekstiilit, wearables) kehittyy turvallisuus- ja tunnistusratkaisuna.

Turvallisuudesta tulee yksille elämäntapa, toisille kapinan sytyke. Tekoälypohjaisia valvontajärjestelmiä käytetään disinformaation lähteiden ja tunnistamiseen ulkopuolelta ja oman blokin sisäisten uhkien tunnistamiseen. Valveutuneet käyttäjät pyrkivät pääsemään maksua vastaan käsiksi vapaampaan tietoon eri reittejä, mutta välinpitämätön enemmistö puolestaan sisäistää turvallisen, suodatetun maailmankuvan. Kriittiset kansalaiset pyrkivät kiertämään rajoitteita hakeutumalla vaihtoehtoisten uutisten perässä epävirallisille, ulkomaisille alustoille. Käyttäjäryhmät voivat näin tiedostamattaan ajautua **heille kohdistetusti suunnitelluille, länsimaisilta näyttäville mutta tietoa kerääville geopoliittisten valtiotoimijoiden tietoa kerääville ja levittäville ulkomaisille alustoille.**

Pinta-ala: Kyberfyysiset linnoitukset AI-valvonnassa

- Kyberpuolustuksen ja hyökkäyksen rajat ovat käytännössä poistuneet, ja geopoliittisen kiristymisen kyberulottuvuudessa tekoälyagentit kamppailevat keskenään, pyrkien vaikuttamaan toistensa ohjelmointiin ja koulutusdataan.
- Länsimaat ovat linnoittaneet yhteiskunnan kriittiset, kytkeytyneet järjestelmät AI-avusteisesti valvottavien, kvanttiturvallisten digitaalisten suojamuurien sisään, joita ylläpitävät suuret teknologiayritykset.
- AI-avusteisen, reaaliaikaisen iskunkestävyyden myötä yhteiskunnan digitaalinen turvallisuus konkretisoituu puolustustekoälyjen infrastruktuuriin, kuten sähkö-, konesali-, satelliitti-, ja kaapelikokonaisuuksiin. Ihmisten valvomat, puolustusagenttien ja AI-järjestelmien pyörittämät *virtuaali-SOCit* yleistyvät.
- Lisääntynyt kytkeytyminen kattaa yhteiskunnan osa-alueet digitaalisista rajavalvontajärjestelmistä tehtaiden OT-järjestelmiin. Softan ja raudan osalta kovetetut järjestelmät nostavat tarpeen kitkeä erityisesti käyttäjälähtöisiä riskejä, social engineeringiä ja sisäpiiriläisyyttä.
- Käyttäjien toimintaa seurataan tekoälyavusteisesti poikkeamien varalta tähän erikoistuneiden yhdysvaltalaisten analytiikkayhtiöiden toimesta sisäisten uhkien tunnistamiseksi. Tietoturvayrityksillä on lisäksi tiedonluovutusvelvoite käyttäjien epäilyttävästä toiminnasta.
- Käyttäjien valvonta kiteytyy hyväksyttyihin ja tietoturvallisiksi katsottaviin älylaitteisiin sisäänrakennettuun takaportilliseen softaan, jonka kautta käytetään digitaalisia peruspalveluita ja mm. henkilökohtaisia AI-assistentteja.
- Käyttäjien velvoitteet pitää laitteensa päivitettyinä ovat korostuneet ja tähän liittyvä valistus on lisääntynyt. Sallittua toimintaa ja laitteita rajataan merkittävästi, mitä käyttäjä ei välttämättä huomaa vallitsevan sensuurin myötä.
- Työntekijöiden sisäänotossa IT-yrityksiin toteutetaan laajaan analytiikkaan ja käyttäytymistietoon perustuvaa seulontaa eri tasoille sopivien tekijöiden tunnistamiseksi. Yksikin virheliike somehistoriassa, valinta-algoritmissa esiintyvä vinouma tai henkilöstä luotu valesisältö voi olla dataa yhdistelemällä tunnistettava työllistymiseste.

Uhat: Valtiotoimijat iskevät kriittiseen infrastruktuuriin

- *Turva-AI:n* valvomia järjestelmiä hallinnoivien digitaalisten ja kyberkaksosten solmukohdat ovat valtiotoimijoiden kyber- ja hybridivaikuttamisen kohteita, joiden kautta hyökkääjät yrittävät poistaa pelistä autonomisen kyberpuolustuksen tason. Järjestelmän urkinnan perusteella voidaan kohdistaa yksittäiseen agenttiin vaikuttamistoimia, joiden kertautuminen alavirtaan läpi muiden agenttien johtaa lumipalloefekteihin. Myös puolustussovellutusten koulutusdatan manipuloiminen on keinovalikoimassa. Ihmisten pitäminen mukana päätöksenteossa ei aina skaalaudu riittävästi, lisäten arvaamattomuutta.
- Yhteiskuntien kyberpuolustusta ylläpitävien energiajärjestelmien älyverkkojen OT-järjestelmät ja reunalaitteet omaavat AI-rajapintojen myötä takaporttiriskejä.
- Kvanttisalausten murtojen myötä paljastamaa historiallista, sensitiivistä käyttäjätietoa hyödynnetään sen kumppaneiden toimesta länsimaissa kriittisten turvajärjestelmien sisällä työskentelevien ihmisten kiristämiseen ja manipulaatioon vakoilu- ja sabotaasitarkoituksessa.
- Lisääntyneen yhteiskunnan valvonnan ja tiedon manipulaation varjolla pyritään autoritaaristen valtioiden ohjaamien haktivistien toimesta radikalisoimaan länsivastaista varjoyhteiskuntaa, joka voidaan mobilisoida infrastruktuureja vastaan ja sisäpiiriläisiksi kriittisiin yrityksiin.
- Satelliitti- ja avaruusohjelmia vakoillaan ja pyritään aktiivisesti sabotoimaan kyberkeinoin blokkien välillä.
- Autonomiseen haavoittuvuuskartoitukseen ja sopivien haitakkeiden rakentamiseen hyökkäystarkoituksessa ohjelmoituja valtiotoimijoiden AI-agentteja voidaan laskea geopoliittisten blokkien offensiivisissa operaatioissa liikkeelle ilman riittäviä pidäkkeitä, johtaen merkittäviin sivuosumiin ja leviämiseen myös omissa toimitusketjuissa.
- Geopoliittisten etupiirien sijaiskonflikteissa nopeasti kehittyneitä, EU-alueella autonomisessa rajavalvonnassa ja poliisitoimessa hyödynnettäviä autonomisia voimankäyttödrooneja pyritään myrkyttämään APT-toimijoiden toimesta.
- Kriittisten toimintojen kytkeytyneisyyden myötä jopa maatalouden automatisoidut komponentit tiloilla toimivista autonomisista laitteista kasvihuoneisiin ovat APT-toimijoille väyliä yhteiskuntien järkyttämiseen.

TRAFICOM

/DATAIMPERIUMIT 2035/

Kehitys ja kytkeytyminen on rajatonta.

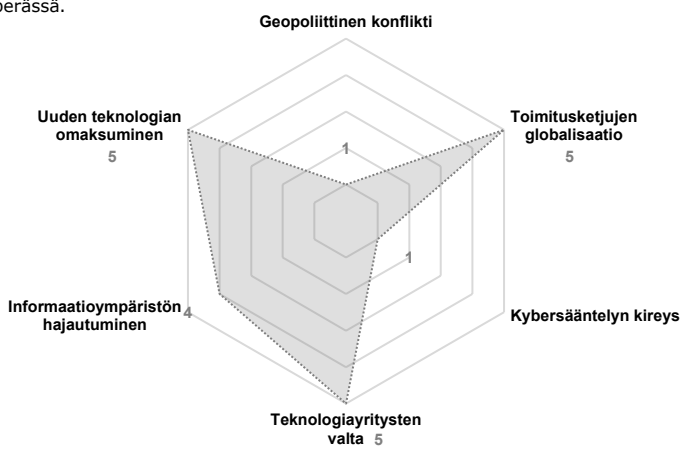
Tekoälymallit ovat yleistyneet monipuolisen datan saatavuuden ja liikkuvuuden myötä. Niiden ympärille rakentuvia Mind²-ympäristöjä ylläpitävät dataimperiumit hallinnoivat käyttäjädataa globaalisti ja tietävät yksilöistä enemmän kuin julkishallinnot tai käyttäjät itse. Merkittävä osa maailman väestöstä nauttii tekoälyjärjestelmiin kytkeytyvistä älykodin mukavuuksista ja **puettavat laitteet ovat yhtä yleisiä kuin älypuhelimet.** Yhdysvaltalaiset yritykset ovat kvanttiteknologian kehityksen kärjessä. **Yritykset ja organisaatiot ovat siirtyneet kvanttilaskennan kestävään salaukseen laajasti dataimperiumien ajettua PQC-algoritmit järjestelmiinsä.** Avaruusteknologia on kilpailun areena tiedustelun, strategisen varustelun ja satelliittipalvelujen kasvavan merkityksen vuoksi.

Ihmiset ovat henkilökohtaisissa peilisaleissaan.

Käyttäjät ovat hakeutuneet suurien palveluntarjoajien kokonaisvaltaista digitaalista elämää tarjoavien**, sensori- ja AI-perustaisten reaaliaikaisten Mind²-ympäristöjen pariin**. Dataimperiumit kilpailevat lukittamalla käyttäjiä ympäristöihinsä. Biometrisen datan luovuttaminen monitorointiin on yleinen portti halvempiin, parempiin ja kohdennetumpiin palveluihin. **Koetut todellisuudet hajautuvat tulotason ja käytetyn ekosysteemin mukaisesti.** Dataimperiumien alustat mahdollistavat ihmisille henkilökohtaiset AI-assistentit ja on demand-sovelluskehityksen, **muovaten kuitenkin samalla niiden kanssa vuorovaikuttavien käyttäjien toimintaa mainostajien ja ylläpitäjien tavoitteiden mukaisiksi.** Luonnollisen kielen rajapintojen ja synteettisen kommunikaation levitessä ihmisten kriittinen ajattelu heikentyy.

Suuryritykset hakevat riippumattomuutta valtioista.

Suuret teknologiayritykset levittävät monopolejaan ja lonkeroitaan. Yhdysvallat on vakiinnuttanut niiden avulla asemansa teknologian ja standardien keskuksena, mutta **poliittinen vaikutusvalta on siirtynyt dataimperiumien kabinetteihin.** Kiinan teknologinen edistys, resurssien ja tuotannon omistajuus ja vaikutuspiiri on ohittamassa sen. Dataimperiumit hyödyntävät AI-kehityksen pönkittämiä asemiaan suurimpien globaalien vuorovaikutusalustojen ylläpitäjinä **vaikuttaen vaaleihin ja politiikkaan ympäri maailman** rakentaakseen itselleen suotuisaa toimintaympäristöä kasvun ja resurssien perässä. EU toimii dataimperiumien asiakkaan roolissa ja normalisoi geopoliittisia suhteitaan kasvun perässä.



Vain dataimperiumit hallitsevat teknologista monimutkaisuutta.

Suurimmat yhdysvaltalaiset teknologiayritykset ovat sementoineet asemansa länsimaissa. Ne onnistuvat välttämään sääntelyn tekemällä itsestään korvaamattomia. Kilpailevat sovellutukset kopioidaan omaan portfolioon tehokkaiden koodiagenttien toimesta tai ostetaan ja vaietaan olemattomiin, ja **EU-yritysten on äärimmäisen vaikeaa tuoda markkinoille omia ratkaisujaan.** Kiinalaiset suuryritykset ovat puolestaan levittäneet vaikutusvaltaansa Digital Belt and Roadin infrastruktuuridiplomatian tuella ja suurin osa maailman ihmisistä on niiden valvontaa ja käyttäytymisdataa keskittävän infrastruktuurin vaikutuspiirissä.

Kasvu edellyttää esteetöntä liikkuvuutta.

Maailmantalouden vakaassa toimintaympäristössä edenneet teknologiset innovaatiot ovat tuoneet toivottua, mutta globaalisti epätasaisesti jakautuvaa kasvua, **vaatien ylläpitoonsa jatkuvasti enemmän ympäristöä kuluttavia resursseja. Dataimperiumit onnistuvat liennyttämään protektionismia ylläpitääkseen kasvulle välttämättömiä vakaita arvoketjuja** ja säilyttääkseen yhteytensä Kiinasta vahvasti riippuvaiseen maailmankauppaan. Venäjä uudelleenintegroidaan maailmantalouteen edullisen energian takaamiseksi. **Yhdysvaltalaisten ja kiinalaisten yritysten ympärillä toimivat teknologiset alihankintaketjut,** joihin ainoastaan niillä itsellään on hallintakyky, **muodostavat kansantalouksien elinehdot.** Valtiot on EU:ta myöten jaettu yritysten ”etupiireihin” pääasiakkuuksien mukaisesti.

Kohoava abstraktiotaso vaikeuttaa sääntelyä.

Sääntely ei pysy suuryritysten teknologiakehityksen vauhdissa. Yhä useammat julkishallinnot ovat kykenemättömiä hallitsemaan monimutkaistuvia digitaalisia ympäristöjä, ja dataimperiumit hyödyntävät asemiaan täyttäen edustajillaan itselleen tärkeimpiä kansallisia ja EU-tason päätöksentekoelimiä. **Parlamentaarinen päätöksenteko on yhä useammin niiden julkishallintojen käyttöön antamien AI-työkalujen sanelemaa.** Palveluntarjoajat pitävät huolta maksukykyisten asiakkaiden datan suojaamisesta, ja huonoiten toimeentulevien kyky nauttia tietoturvasääntelyn perustasosta on heikentynyt. **EU on heikentynyt poliittisena toimijana ja sääntelijänä,** mutta viranomaisyhteistyö on tiivistynyt tavallisten kansalaisten turvaamisessa kyberrikollisuudelta siellä, minne dataimperiumien kiinnostus ei yllä.

Suuryritykset hakevat riippumattomuutta valtioista

Suuret teknologiayritykset levittävät monopolejaan ja lonkeroitaan kaikkialla maailmassa erityisesti AI-kehityksen tukemana. Yhdysvallat on säilyttänyt niiden myötävaikutuksella asemansa teknologian ja standardien keskuksena. Kiinan teknologinen edistys, resurssien ja tuotannon omistajuus on kuitenkin kasvanut, sen sovellutukset dominoivat maailmalla ja vaikutuspiiri kasvaa liittoumissa. **Dataimperiumit onnistuvat liennyttämään Yhdysvaltojen ja Kiinan vastakkainasettelua ylläpitääkseen vakaita arvoketjuja** ja Kiinasta riippuvaista maailmankauppaa kasvun ylläpitämiseen. Poliittista vaikutusvaltaa on siirtynyt länsimaissa vaihtokaupassa demokraattisesti valituilta päätöksentekijöiltä ***dataimperiumien*** kabinetteihin, joissa poliitikot vaihtavat julkishallinnon resursseja, suotuisaa sääntelyä ja kansainvälistä vaikutusvaltaa statukseen ja vaalirahaan.

Maailmantalouden suhteellisen vakaassa toimintaympäristössä edenneet teknologiset innovaatiot ovat tuoneet toivottua, mutta globaalisti epätasaisesti jakautuvaa kasvua, vaatien ylläpitoonsa samalla jatkuvasti enemmän ympäristöä kuluttavia resursseja. **Dataimperiumit hyödyntävät Yhdysvaltojen ulkopolitiikkaa rakentaessaan itselleen suotuisaa toimintaympäristöä, etsien kasvun mahdollisuuksia ja resursseja ensisijaisesti mielipidekampanjoilla ja tarvittaessa välillisin voimakeinoin.** Ne hyödyntävät tekoälykehityksen pönkittämiä asemiaan suurimpien globaalien vuorovaikutusalustojen ylläpitäjinä ajaakseen valtioita irti markkinoita häiritsevästä nationalismista, vaikuttaen vaaleihin ja politiikkaan ympäri maailman.

EU on tuonut 2020-luvulla toteutetun sääntelyn 2030-luvulle ja vaatii alueella toimivilta **yrityksiltä korkeampia turvallisuusstandardeja**, kuin mitä Yhdysvallat on valmis hyväksymään. Dataimperiumit protestoivat tätä uhaten rajoittaa teknologioiden saatavuutta, ja **EU joutuu taipumaan mm. AI-sääntelyn keventämiseen.** Talousintressit ja huoli maanosan kilpailukyvystä ajaa kiilaa jäsenmaiden välille, saaden niiden intressit erkanemaan voimakkaasti, heikentäen yhteistä päätöksentekokykyä.

Kasvu edellyttää esteetöntä liikkuvuutta

EU ei kykene yhtenäiseen infrapolitiikkaan kiinalaisten ja yhdysvaltalaisten suuryritysten jakaessa markkinoita ”etupiireihinsä”. Yhdysvaltojen palvelut ja toimitusketjut koetaan toisaalta epäluotettavina, kun niitä on käytetty toistuvasti geopoliittisena vipuvartena 2020-luvulla. Kiina käyttääkin tilaisuutta hyväkseen, tarjoten länsimaiden käyttöön edistyksellisempää teknologiaa yhdysvaltalaisen tilalle.

Dataimperiumit haalivat itselleen jatkuvasti lisää dataa, laskentatehoa ja uusimpia siruja, pitäen hinnat ja uusimmat sovellutukset saavuttamattomissa pienemmiltä toimijoilta. Ne ovat hyödyntäneet keräämänsä datan ohjelmistokehityksen monopolisointiin AI-koodiagenttiensa välityksellä. EU päättää tasapainoilla suurvaltojen palveluntarjoajien välillä **hakien taloudellisen pragmaattisuuden ja turvallisuusharkinnan keskitieltä parhaita ratkaisuja niin Yhdysvaltojen, kuin Kiinankin markkinoilta.**

EU on kehityksessä takamatkalla, eikä halua lukittautua pois mistään verkostoista hakiessaan teknologisen kehityksen tarjoamia kasvun paikkoja. **Käytännössä EU:n kriittisin pilvi-infrastruktuuri on edelleen eurooppalaista tai yhdysvaltalaista, mutta esimerkiksi kuluttajapuolella on käytössä paljon kiinalaista infrastruktuuria ja sovellutuksia.**

Harva hallitsee teknologista monimutkaisuutta

Dataimperiumien valta ja vauraus on rakentunut jatkuvan kasvun, uusimpien teknologisten ratkaisujen vaatimien monimutkaisten toimitusketjujen, resurssien ja energian keskittämistarpeen varaan. Yhteiskuntien palveluntarjonta on keskittynyt AI-kehityksen myötä niiden datainfrastruktuurein skaalaetujen mukaan. Yhdysvaltalaisten ja kiinalaisten suuryritysten ympärillä toimivat alihankintaketjut, joihin ainoastaan niillä itsellään on kokonaiskuva ja hallintakyky, muodostavat käytännössä asiakkaina toimivien kansantalouksien elinehdot.

Erityisesti Yhdysvaltojen AI-palveluita rakentaneet yritykset ovat onnistuneet sementoimaan vaikutustaan kuluttajien ja lainsäätäjien toimintaan ja päätöksentekoon kaikissa länsimaissa. Ne onnistuvat ehkäisemään sääntelypyrkimyksiä pysyttelemällä teknologisen kehityksen eturintamassa, levittäen lonkeroitaan yhteiskunnissa, ja tehden itsestään korvaamattomia. Ohjelmointiautomaation AI-avusteiset edistysaskeleet ovat keskittäneet vaikutusvaltaa entisestään suurimmille hyperskaalaajille. Heikentynyt kilpailuasetelma on näivettänyt käyttäjän näkökulmasta useaa palvelua merkittävästi, ja uudet kilpailijat pyrkivätkin aktiivisesti haastamaan dataimperiumien monopoleja. **Uusiin innovaatioihin kohdistuu kuitenkin suoraa vakoilua kun kehitystyötä tehdään dataimperiumien omilla alustoilla;** mahdollisten kilpailijoiden teknologioita hyödynnetään omassa portfoliossa tai ostetaan ja vaietaan olemattomiin omien ratkaisujen aseman suojelemiseksi. EU-yritysten on vaikeaa tuoda markkinoille omia ratkaisujaan. **Data residency sijaitsee suuryritysten emomaissa.**

Kiinalaiset suuryritykset ovat levittäneet vaikutusvaltaansa erityisesti globaalin etelän maissa Digital Belt and Roadin infrastruktuuridiplomatian tuella. Suurin osa maailman ihmisistä on niiden valvonnan ja käyttäytymisdatan keskittämiseen hyödynnettävien sovellutusten ja infrastruktuurin suorassa vaikutuspiirissä. Ne estävät Kiinan valtion tuella länsimaisten yritysten leviämistä etupiiriinsä, pyrkien ottamaan niiltä markkinaosuutta myös demokratioissa kehystämällä palvelunsa valtiolle ja yhteiskunnalle *arvokkaan elämän* mahdollistavana vaihtoehtona lännen *yksityiselle valvontakapitalismille*.

Kohoava abstraktiotaso vaikeuttaa sääntelyä

Sääntely ei pysy suuryritysten teknologiakehityksen vauhdissa ja **yhteiskuntien digitalisaatio ja tehostaminen sivuuttaa itsetarkoituksena kansallisvaltion tehtävien toteuttamisen.** Yhä useammat julkishallinnot ovat kykenemättömiä hallitsemaan monimutkaistuvia digitaalisia ympäristöjä, ja dataimperiumit alkavat hyödyntämään sääntelytyhjiötä **pyrkien täyttämään edustajillaan tai palkollisillaan itselleen tärkeimpiä kansallisten ja EU-tason päätöksentekoelimiä. Kokiessaan sääntelyn uhkaavan valtaa ja liiketoimintaa ne toteuttavat tehokkaita mielipidekampanjoita ja lobbausta** saadakseen tahtonsa läpi. Parlamentaarinen päätöksenteko ja perusteet ovat yhä useammin niiden AI-työkalujen sanelemia; tekoälytuotoksia vertautetaan asiantuntijatietoon ja kuulemisia vähennetään.

EU on heikentynyt poliittisena toimijana, mutta viranomaisyhteistyö on tiivistynyt operatiivisessa toiminnassa kansalaisten turvaamisessa kyberrikollisuudelta. **Palveluntarjoajat pitävät huolta maksukykyisten asiakkaiden datan suojaamisesta, ja huonoiten toimeentulevien kyky nauttia tietoturvasääntelyn perustasosta on heikentynyt.**

Uuden teknokratian aidat rakennetaan AI-skaala edellä

Tekoälymallit ovat yleistyneet globaaleissa tietoverkoissa monipuolisen datan saatavuuden ja liikkuvuuden myötä. Niiden ylläpitäjät hallinnoivat käyttäjädataa globaalisti ja tietävät yksilöistä enemmän kuin julkishallinnot tai käyttäjät itse. **Demokratioiden päätöksentekoa on siirtynyt algoritmiohjaukseen hallinnon uusien käyttöliittymien myötä.** AI-järjestelmät sisältävät yleensä dataimperiumeille aukeavia takaovia tai eivät ole viranomaisten auditoitavissa. Autonomisen teknologian siirtyminen mustiin laatikoihin **tekee vaikeammaksi arvioida sovellutusten ja agenttien perimmäisiä käyttötarkoituksia sekä niihin liittyviä vastuu-, turvallisuus-, ja yksityisyyskysymyksiä.** Alustat voivat myös suurvaltojen myötävaikutuksesta tai yhteistyössä paikallishallintojen kanssa estää sisältöä, ohjata mielipiteitä tai tehdä taloudellista painostusta määrätyllä alueella.

Vendor lock-ilmiö on kiihtynyt **suuryritysten omien koodiagenttien kaivautuessa organisaatioiden toimitusketjuihin rakentamaan itse järjestelmiä, jotka sopivat vain tietyn organisaation toimitusketjuun. Dataimperiumit estävät toistensa agenttien toimintaa rajaamalla niiden oikeuksia, ja rakentavat rajapintoja vain omien yhteistyökumppaneidensa kanssa.** Ohjelmointi keskittyy hyperskaalaajille, kun autonomiset koodiagentit hitsaavat järjestelmien väliset palat yhteen optimoiden toimintaa reaaliaikaisesti mm. kyberfyysisissä ympäristöissä. Järjestely mahdollistaa itseoppivuudellaan toimitusketjujen ketterän uudelleenreitittämisen vikatilanteissa. **Koodiagenttien käyttöönoton seurauksena on laajaa työttömyyttä vailla koordinoituja ohjelmia seuraamusten hallintaan, ja eriarvoistumiskehitys kiihtyy.**

Kvantti-innovaatioiden perässä

Tekoälyjärjestelmien vakiinnutettua asemansa yhteiskunnissa puolijohderatkaisuja energiatehokkaampi kvanttilaskenta herättää dataimperiumien kiinnostuksen, jotka pyrkivät **yhdistämään kvanttialgoritmeja koneoppimisohjelmiin.** QCaaS–palveluiden kvanttilaskenta on tuonut merkittäviä etuja lääke- ja logistiikkasektoreilla. **Yhdysvaltalaiset yritykset ovat kehityksen kärjessä lisättyään EU-alueen yritysten kyvykkyyksiä portfolioonsa kiinalaisten pysytellessä kannoilla.** Organisaatiot ovat siirtyneet kvantinkestävään salaukseen dataimperiumien PQC-algoritmien käyttöönoton myötä.

Rajaton kasvu ja kytkeytyminen vaativat resursseja

Suurimmat tekoälysovellutukset ovat törmänneet julkisen koulutusdatan ehtymiseen. **Ratkaisuna seuraavaan askeleeseen dataimperiumien moninaiset palvelut niputetaan yhden käyttöliittymän ”yhteisaivoiksi”, (*Mind*²), joiden yhteyteen käyttäjät kytkeytyvät puettavalla teknologialla ja biometrisillä siruilla.** Käyttöliittymä kerää koulutustarpeisiin AI-agenttien välityksellä dataa interaktioista ja elintoiminnoista, muodostaen ”kollektiivista”, reaaliaikaista ymmärrystä käyttäjien välillä. **Merkittävä osa maailman väestöstä nauttii älykodin mukavuuksista ja puettavat laitteet ovat yhtä yleisiä kuin älypuhelimet.** 6G-verkko yhdistää satelliitit, lennokit, maanpäälliset tukiasemat ja IoT-laitteet saumattomaksi kokonaisuudeksi. Verkon ohjaus perustuu resursseja reaaliaikaisesti optimoivaan tekoälyyn ja koneoppimiseen. **AR-VR- ja metaversumiympäristöt toimivat viiveettömästi.**

Dataimperiumien yhteisaivot ulokkeineen rakentuvat valtavalle fyysisen maailman infrastruktuurille, ja sen jatkuvasti vaatimalle energialle ja komponenteille. Kasvua haetaan energiamuodosta riippumatta ja ilmastosta välittämättä. **Avaruusteknologia on merkittävä yrityskilpailun areena** tiedustelun, strategisen varustelun ja satelliittipalvelujen kasvavan merkityksen vuoksi. **Laskentakapasiteettia viedään datakeskussatelliiteilla kiertoradalle,** paneeliteknologian kehityksen taatessa satelliiteille paremman energiansaannin. Dataimperiumien kasvu edellyttää mineraaleja, ja **asteroidilouhintateknologiaa kehitetään raaka-ainevirtojen takaamiseksi.**

Manipulaation maailmasta pääsee eroon maksukyvyllä

Nopealla AI-kehityksellä ja synteettisten sisällöntuottajien kytkeytymisellä alustoihin on ollut hintansa ja julkinen internet on täyttynyt vaikeasti kontrolloitavalla digitaalisella saasteella. Seurauksena **käyttäjät ovat hakeutuneet tekoälyassistenttien ja AI–kuratoinnin laadunvalvomiin suurien palveluntarjoajien *Mind²-superapplikaatioympäristöjen* pariin.** Ympäristöt tarjoavat ihmisille toimivan ja turvallisen digitaalisen olemassaolon kokemuksia ja vertaistodennettuja tiedonlähteitä eri hintaluokissa. Ajattelu muovautuu ”yhteisaivojen” välityksellä ja vaikutuksesta, ja maksukyky määrittää pääsyä parhaaseen ymmärrykseen.

Yhtenäinen näkemys maailmasta jää 2020-luvulle. Dataimperiumit ovat sittemmin aidanneet yksityistä ja julkista tietoa sekä käyttäjiä vain niille itselleen saatavilla oleviin, kokonaisvaltaisiin informaatioympäristöihin. Koetut todellisuudet **hajautuvat tulotason ja käytetyn AI-ekosysteemin mukaisesti.** Premium-tason käyttäjät maksavat muovaavat infoympäristöjä toiveidensa mukaisiksi erottuen eliittinä. **Yritykset pyrkivät saavuttamaan erityisesti näiden ”korkean arvon käyttäjien” arvostuksen, ja heidän tietoturvastaan huolehditaan.** ”Tietokeskiluokka” valitsee yksilölliseen ja personoitavaan assistenttiavusteiseen algoritmiohjaukseen perustuvan kokonaisvaltaisen elämäntavan metaversumeineen. AI-ympäristöjen ulkopuolelle jättäytyneet suosivat yksittäisiä maksumuurimedioita tai hakeutuvat Darkwebin ja muiden vaihtoehtoympäristöjen puolelle etsimään *”totuutta”*. Alati mukautuvan luonnollisen kielen ja inhimillisen synteettisen kommunikaation yleistyessä **kriittinen ajattelu heikentyy, vahvistaen ihmisille syötettävien ajatusten voimaa.**

Pienet valtioblokit pystyvät verifioimaan luotettavaa tietoa sisäisesti, **mutta isossa kuvassa tiedonhallinta ei enää ole dataimperiumien toteuttaman digitaalisen yhteismaan aitaamisen myötä mahdollista.** Valtionhallinnoissa keskitytään informaatioon, joka voidaan reaalimaailmassa vahvistaa faktaksi.

Ihmiset ovat henkilökohtaisissa peilisaleissaan

Dataimperiumit lukittavat mahdollisimman paljon käyttäjiä alustoilleen ja ympäristöihinsä keräämään heistä yhä enemmän dataa ja ohjaamaan käyttäytymistä. Teknologiasta tulee uskonnon kaltainen elämäntapa, jossa algoritmien ohjaama elämä on tavoiteltava tila. **Tiedon luovuttamiselle on käytössä jatkuvia rajapintoja tekoälyassistenteista sensoreihin**. Yritykset kehittävät vauhdilla LBM (*large behavior models*) –ratkaisuja, jotka perustuvat puettavan teknologian sensoreihin. Sensorit ja laitteet kytkeytyvät eri maksutasojen superapplikaatioympäristöihin parantamaan palvelujen personointia. Biometrisen datan luovuttaminen monitorointiin on yleinen portti halvempiin, parempiin ja kohdennetumpiin palveluihin, joita voi generoida dataimperiumien sovelluskaupan ja henkilökohtaisen assistentti-agentin välityksellä.

Freemium-käyttäjät toimivat mainonnan ja bottien vaikutuksen kohteina, luovuttaen dataansa palveluita vastaan. **Tekoälyassistenttien ilmaisversiot toimivat henkilökohtaisina seuralaisina, muovaten kuluttajien käyttäytymistä** mainostavien yritysten tavoitteiden mukaan. Ilmaiskäyttäjien generoimat sovellutukset sisältävät syvällisesti personoituja mainoksia. Käyttäjät alkavat manipulaation seurauksena toisintamaan koneälyjen ominaisuuksia, mutta korkeampiin maksuluokkiin sisältyy uniikkien piirteiden korostamista, inhimillisyyden kokemuksia ja itse generoitujen sovellusten parempaa räätälöintiä.

Dataimperiumit eristävät ihmisiä kansallisvaltioistaan ja muista yhteisöistään, siirtäen heidän kognitionsa omiin rajapintoihinsa ja käyttöliittymiinsä tuottavimmilta osin. Darkwebiä ja vaihtoehtoyhteisöjä hyödynnetään aktiivisesti pakopaikkoina digitaalisen maailman täysnäkyvyydeltä. Elämän siloteltu digitaalinen taso elämän käyttöliittymineen on vahvassa kontrastissa **fyysisen maailman sään ääri-ilmiöiden, lisääntyvän pakolaisuuden, eriarvoistumisen ja paikallisten resurssikonfliktien yhä enemmän piinaaman ympäristön kanssa.**

Pinta-ala: Kytkeytyminen käy ylikierroksilla

- Keskeisimpinä turvallisuuden tuottajina toimivat dataimperiumit keskittävät merkittävästi resursseja suojellakseen tärkeimpiä, Mind²-kokonaisuuksien tietovarantoja. Ne kerryttävät liikesalaisuuksikseen myös parhaita tietoturvakäytäntöjä ja löydettyjä heikkouksia. Teknologiajäteillä on tekoälyn avulla yhä parempia tapoja torjua perinteisiä hyökkäyksiä, mutta motivaatio suojata muita, kuin omia premium-käyttäjiä ja järjestelmiä on vähäistä.
- Lisääntynyt kytkeytyneisyys on lisännyt kyberrikollisten mahdollisuuksia ulottaa vaikutustaan käyttäjien elämään intiimillä tasolla. Laitteilla täydennetyn arjen toimivuus on riippuvaista monenlaisista persoonaan kytkeytyvistä, haavoittuvuuksia lisäävistä rajapinnoista ja laitteista.
- AI:n laaja integroiminen ydinliiketoimintoihin on keskittänyt organisaatioissa sensitiivistä dataa erikoistuneihin järjestelmiin, tehden niistä houkuttelevia kohteita. Kansalaisia profiloidaan elämän käyttöliittymissä entistä tarkemmin, yksityisyydensuojaa voi hankkia luksustuotteena. Pk-yrityksillä on ongelmia tietonsa suojaamisessa, kun turvallisesta datankäsittelystä on tullut kallista.
- Valtiotoimijat keskittyvät kyberulottuvuudessa kyberrikollisuuden kitkemiseen kansainvälisessä yhteistyössä ja tuomaan kyberturvallisuutta sinne, minne dataimperiumit eivät ole ulottaneet toimintaansa. APT-toimijat keskittyvät urkintaan ja teollisuusvakoiluun emovaltion yritystoiminnan hyväksi.
- Teknologisen kehityksen kyydistä jäänyt sääntely on heikentänyt dataimperiumien ekosysteemien ulkopuolelle jääneiden oikeutta tietosuojaan ja -turvaan. Kyberrikolliset ulottavat toimintaansa alueille, minne niillä ei ole taloudellista motivaatiota tai sääntelyn velvollisuutta levittää turvaverkkojaan.
- Yritykset syyttävät valtioita teknologian politisoinnista ja korostavat suojaavansa käyttäjiään peittäen näkyvyyttä toimintaansa.
- Kytkeytymisen myötä kaiken ohjelmoinnin ja koodin vertailukohdan muodostavat dataimperiumien jatkuvasti päivittyvät, reaaliaikaiset datamassat, joiden varaan tekoälyagentit rakentavat autonomisesti järjestelmiä. Historiallista tietoa, vanhoja verkkosivuja ja sisältöjä sekä parhaita käytäntöjä on vaarassa kadota.

Uhat: AI-dataifikaatio johtaa rikollisuuden uusiin muotoihin

- Dataimperiumien toimitusketjujen moninaiset alihankkijat ovat kyberrikollisten ensisijaisia kohteita niiden kerryttämän personointitiedon varastamiseksi.
- Mind²-käyttöliittymiä ja palveluja imitoivia koodiagenttien avulla luotuja, mikrokohdennettuja valeversioita lasketaan rikollisten toimesta liikkeelle käyttäjätietojen varastamiseksi. Sensorien ja pinta-alan kattaessa digitaalisen elämäntavan yleistyneistä kotiroboteista AI-assistentteihin ja biometrisiin siruihin, tietojen yhdistely mahdollistaa virallisilla alustoilla täydestä menevien ihmisten virtuaalikopioiden luomisen monenlaisiin rikollisiin tarkoituksiin.
- Esimerkki: Mind²-ympäristöissä yleistyneet lifestyle-käyttöliittymät ovat kerryttäneet tietoa premium-käyttäjien käyttäytymisestä ja paikkatiedosta, ja tietokantojen murtaminen mahdollistaa kyberhyökkäysten personoinnin. Tietoja myydään Darkwebissä. Premium-käyttäjien tilejä kloonaamalla pyritään toisaalta pääsemään dataimperiumien varakkaiden käyttäjien lähelle huijaustarkoituksissa.
- Hyökkääjät voivat murtaa jopa dataimperiumien turvajärjestelyt hyödyntämällä yllättäviä hyökkäysvektoreita, kuten vanhentunutta tietoa ja nollapäivähaavoittuvuuksia, joita itseoppivat järjestelmät eivät ole nähneet koulutusdatassaan. Vanhoihin ohjelmistokirjastoihin perustuva injektiohyökkäys voi kohdistua toimitusketjun legacy-järjestelmien kautta koodiagentteihin, romahduttaen koko toimitusketjun.
- Alustayhtiöiden edistyneet suojausmekanismit, informaatioympäristön moderointi sekä onnistuneiden hyökkäysten tekemisen kustannusten kasvu ovat johtaneet vaikuttavan ja näkyvän haktivismin katoamiseen. AI-elämäntapaa vastustavat aktivistit ja uskonnolliset tahot hyökkäävät fyysisesti infrastruktuuria vastaan fyysisenä sabotaasina. Sitä vastaan hyökätään myös laskennan rakentamisen myötä *resurssi-imperialismista* kärsineiden aktivistien toimesta maantieteellisillä kriisialueilla. Seurauksena on yhteiskunnan kriittisten palvelujen yllättävää lamautumista.
- Tekoälykehityksen vaikutus on ilmentynyt lisääntyvinä IT-alan irtisanomisina, mikä on lisännyt merkittävästi sisäpiiriläisyyden uhkaa. Darkwebissä pyritään rekrytoimaan dataimperiumien ex-työntekijöitä rikollisiin organisaatioihin.

Jos sen voi kuvitella, siihen voi varautua.

Traficomin teknologia- ja strategiatoiminto

ennakointi@traficom.fi

Kirsi Karlamaa, Teknologia- ja strategiajohtaja
Aleksi Blomqvist, Erityisasiantuntija
Paul Hermansson, Erityisasiantuntija
Henri Jokinen, Erityisasiantuntija
Markus Mettälä, Erityisasiantuntija