



Cyberwatch Finland

MAGAZINE 3/2026

Kybervarmuus 2027



Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

Tavoitteena kyberkyvykkäämpi maailma



SISÄLTÖ



4

Pääkirjoitus
Kybervarmuus
– tulevaisuuden ratkaisut
➤ **AAPO CEDERBERG**



6

Digitaalinen suvereniteetti
voidaan menettää tai
saavuttaa arkisilla
ratkaisuilla
➤ **REPE HARMANEN**



10

Kyberturvallisuuden
rahoitus ja yritysten
toimintaympäristö
ratkaisevat Suomen
turvallisuuden
➤ **RISTO RAJALA
& PETER SUND**



14

Datamyrkytys
ja RAG-myrkytys
➤ **KIMMO K. KASKI**



21

Vaativuuden mukaisuus
energiajärjestelmän
reunalla
➤ **TIIVISTELMÄ CYBERWATCH
FINLANDIN JULKAISEMASTA
WHITE PAPER RAPORTISTA
LOKAKUU 2026**



27

Cyberwatch Finland

KUUKAUSIKATSAUS
LOKAKUU/2026
➤ Cyberwatch Finland liittyi osaksi Netum Groupin 21.4.2026.



42

Netum & Cyberwatch
KYBERVARMUUS

Cyberwatch MAGAZINE

JULKAISIJA
Cyberwatch Oy
Kansakoulukatu 1b, Helsinki, Finland

TOIMITUS
Päätoimittaja Aapo Cederberg
aapo@cyberwatchfinland.fi

TAITTO
PuulaMedia / Mari Riepponen

KUVAT
AdobeStock, **AI GENERATED**

PAINO
Scanseri Oy, Helsinki

ISSN 2490-0753 (print)
ISSN 2490-0761 (web)



Kybervarmuus – tulevaisuuden ratkaisut

Kyberhyökkäysten määrä on kasvanut viime vuosina keskimäärin 30 prosenttia vuosittain. Tekoälyn käyttö hyökkäyksiin on muuttanut hyökkäystekniikoita sekä nopeuttanut niiden suunnittelua ja toteuttamista. Haavoittuvuuksien löytäminen on huomattavasti nopeampaa, ja räätälöity kyberhyökkäys voidaan toteuttaa minuuttiluokassa uuden haavoittuvuuden havaitsemisesta. Venäjän APT-ryhmät ovat viimeisen vuoden aikana hyödyntäneet tekoälyä 90 prosentissa kyberoperaatioistaan. Tekoäly ei ole pelkästään valtiollisten uhkatoimijoiden käytössä, vaan se läpileikkaa koko uhkatoimijoiden kirjon.

Meidän on ymmärrettävä, että haaste kasvaa ja peli kovenee. Tulevaisuuden kyberpuolustuksen on

myös pystyttävä hyödyntämään tekoälymallien tarjoamia mahdollisuuksia samalla kuitenkin noudattaen kasvavaa tekoälyn käyttöön liittyvää regulaatiota. Meidän on opeteltava tekoälyn vastuullinen käyttäminen kaikilla kyberpuolustuksen osa-alueilla, uhkatiedustelussa, havainnointikyvyn parantamisessa, suojaamisessa ja palautumisessa. Uutena toimintatapana aktiivisen kyberpuolustuksen eli hyökkäyksellisen kybertoiminnan on oltava osa modernia kyberpuolustusta. Kybermaailman ”kaukovaihtaminen” on välttämätöntä, jotta hyökkääjien kapasiteettia ja suunnitelmia voidaan heikentää aktiivisesti. Uhkatiedustelun on mahdollistettava meille oikea-aikainen ja ennakkoiva tilannekuva.

Euroopassa panostetaan tulevana vuosina perinteisen sotilaallisen puolustuksen kehittämiseen, mikä on välttämätöntä ja järkevää. Kyberpuolustuksen merkitys on kasvanut sotilaallisten operaatioiden yhtenä kriittisenä osatekijänä, mutta ennen kaikkea siviiliyhteiskunnan toiminnan takaajana. Sotien ja eriateisten kriisien vaikutus kohdistuu entistä enemmän yhteiskunnan kriittisiin toimintoihin ja infraan. Sodan kynnyksen alapuolelle jäävien kyberhyökkäyksien määrä on hybridisodankäynnin kokonaisuudessa eniten kasvanut osa-alue.

Yhteiskuntamme kehitys ja kasvu perustuvat hyvin toimiviin digitaaliin palveluihin. Niiden toimivuus on pystyttävä turvaamaan kaikissa tilanteissa ja erityisesti kriisitilan-

teissa. Kybervarmuuden merkitys korostuu, ja meidän on jatkossa kehitettävä digitaalisia palveluita ja kyberturvallisuutta yhtenä harmonisena kokonaisuutena. Kyse ei ole pelkästään teknologiavalinnoista, vaan ennen kaikkea kokonaisuuden hallinnasta. Tiedämmekö oman kyberkypsyytemme tason ja pystymmekö tunnistamaan kyberriskit? Kyberlain-säädännön edellyttämä organisaation johdon keskeinen rooli ja tilanneymärrys sekä kyky riskipohjaiseen päätöksentekoon nousevat jatkossa arvoon arvaamattomaan. Mitään uusia ”temppuja” ei tarvita, vaan systemaattista työtä oman organisaation kybervarmuuden parantamiseksi.

Tekoälyn käyttö kyberhyökkäykseen luo uusia haasteita ja uhkakuvia.

Datan merkitys korostuu, koska sen perusteellahan tekoäly toimii ja ”ajattelee”. Olemme jo pitkään puhuneet datan manipuloinnista, jota tapahtuu jatkuvasti. Uutena salakavalana ilmiönä nousee datan myrkyttäminen, joka voi johtaa esimerkiksi tutkimustulosten vääristymiseen ja toiminnanohjausprosessien virheisiin, joilla voi olla kohtalokkaat seuraukset yhteiskunnan kriittisissä toiminnissa. Tässä lehdessä on professori Kimmo Kasken erinomainen artikkeli tästä uudesta ilmiöstä, johon joudumme kaikki jatkossa perehtymään.

Kaikesta huolimatta kyberturvallista loppuvuotta! Muistetaan huolehtia oman organisaatiomme kybervarmuudesta ja sen jatkuvasta parantamisesta.



AAPO CEDERBERG
Liiketoimintajohtaja
Netum - Cyberwatch

Digitaalinen suvereniteetti voidaan menettää tai saavuttaa arkisilla ratkaisuilla

> REPE HARMANEN,
NETUM GROUP OYJ

Suomi on vaarassa menettää digitaalisen suvereniteettinsa päätöksillä, joita ei pidetä päätöksinä. Tuttu viestintäsovelus, ohjelmisto tai pilvialusta otetaan käyttöön nopeasti ja tarve kilpailutukselle huomataan, kun data on jo siirretty. Sen jälkeen ei enää kilpailuteta teknologiaa, vaan sitä, kuka saa myydä pääsyn jo valittuun teknologiaan. Ja samalla on huomaamatta alistettu oma data EU:n ulkopuolisen valtion lainsäädännölle.

Vuonna 2025 Kilpailu- ja kuluttajavirasto totesi, ettei VR noudattanut erityisalojen hankintalakia hankkiessaan vuonna 2023 pilvipalveluita ja niihin liittyviä asiantuntijapalveluita kuudessa kokonaisuudessa, joiden yhteisarvo ylitti kolme miljoonaa euroa. VR perusteli osaa hankinnoista sillä, ettei laissa määritelty kynnysarvo ylittynyt, ja osaa sillä, että palvelun saatavuudelle oli tekninen tai yksinoikeuteen liittyvä peruste.¹

Ongelman taustalla oli VR:n IT-arkkitehtuuri, joka oli rakentunut teknologiajätti Amazon Web Servicen infrastruktuurin varaan. Yhtiön KKV:lle antaman selvityksen mukaan toiseen pilviteknologiaan siirtyminen olisi vaatinut koko arkkitehtuurin uudelleenrakentamista, mikä puolestaan edellyttäisi, että osa VR:n digitaalisista sovelluslähdekoodista olisi kirjoitettava uudelleen. KKV ei pitänyt tätä riittävänä perusteena sille, että VR ei ollut noudattanut hankinnoissaan lakia.²

Käytännössä VR oli siis tehnyt teknologiavalintansa jo vuosia aikaisemmin ja rakentanut IT-infrastruktuurinsa siitä riippuvaiseksi. Sitä ei vain ollut koskaan käsitelty päätöksenä.

VR ei ole ainoa vastaavan kaltaisen valinnan tehnyt hankintayksikkö ja nyt sama kehitys näkyy myös tekoälyssä. Organisaatiot ottavat kovaa vauhtia käyttöön kaupallisia kielimalleja ja tekoälyavustajia, rakentavat niiden ympärille työkaluja ja kouluttavat henkilöstönsä käyttämään niitä. Harvassa organisaatiossa tätä käsitellään alustavalintana, vaikka kyse on juuri siitä. Ja kuten VR:n tapauksessa, tällaiset alustavalinnat johtavat digitaalisiin riippuvuussuhteisiin, joiden purkaminen maksaa.

Digitaalinen riippuvuus on koko Euroopan ongelma

Pilvipalveluiden, samoin kuin tekoälypalveluiden, markkina on vahvasti muutaman suuren toimijan käsissä.

Euroopan komission mukaan EU:n omien pilvipalveluntarjoajien osuus Euroopan markkinasta laski 29 prosentista vuonna 2017 noin 15 prosenttiin vuonna 2022 ja on sen jälkeen pysynyt samalla tasolla. Kolme EU:n ulkopuolista teknologiajättiä hallitsee yli 70 prosenttia markkinasta.⁶

Olemme kaikki käytännössä riippuvaisia pääasiassa yhdysvaltalaisista palveluntarjoajista. Etenkin nykyisessä geopolittisessä ympäristössä tämä on ongelmallista.

Euroopan komissio vastasi tilanteeseen kesäkuussa 2026 julkaisemalla teknologiasuvereniteettiin tähtäävän strategiapaketin, johon kuuluu myös eurooppalaisten pilvi- ja tekoälypalveluiden kehittämistä tukeva lakiehdotus Cloud and AI Development Act (CADA) ⁵.

CADA määrittelee julkisen sektorin pilvipalveluille neljä eri tasoa, joiden kautta niiden suvereniteettia voitaisiin arvioida:

1. Palvelun prosessoima ja tallentama data sijaitsee fyysisesti EU:n alueella.
2. Palveluntarjoajan pitää pystyä osoittamaan olevansa riippumaton EU:n ulkopuolisista valtioista ja ohjelmiston toimitusketjun tulee olla läpinäkyvä.
3. Palveluntarjoajan omistuksen tulee olla EU:ssa, sen täytyy noudattaa EU:n sääntelyä ja täyttää muita kriteerejä esimerkiksi henkilöstön kansalaisuuksiin liittyen.
4. Palveluntarjoajan ohjelmiston tulee olla täysin tämän hallinnassa ja läpinäkyvä siten, että EU:n ulkopuolisilla mailla ei ole mahdollisuutta puuttua sen toimintaan millään tavalla.

Paketin julkistuksen yhteydessä komission varapuheenjohtaja **Henna Virkkunen** viittasi riskiin, jossa ulkopuolisella toimijalla voisi olla Euroopan kriittisiin palveluihin niin sanottu ”kill switch”. Tämä olennainen ajatus on digitaalisen suvereniteetin ytimessä. Digitaalisessa suvereniteetissä jokaisen digi-

taalisen infrastruktuurin osasen ei tarvitse olla eurooppalainen, mutta kriittisten palvelujen toimivuus ei saa olla riippuvainen sellaisen tahon yksipuolisesta päätöksestä, jota EU ei hallitse.⁷

Millään taholla ei saa olla kill switchiä eurooppalaisiin yhteiskuntiin.

Ranska on muuttanut ajatuksen lain-säädännöksi

Ranskassa ajatusta sovelletaan jo käytännössä. Valtion pilvipalvelujen käyttöä on ohjannut vuodesta 2021 Cloud au centre -doktriini eli periaatepäätös, joka ohjaa vahvasti näiden palvelujen digitaaliseen suvereniteettiin. Doktriini esimerkiksi teki kaupallisille digitaalisille palveluille myönnettävästä SecNumCloud-vaatimusstandardista pakollisen, mikäli palvelussa käsitellään valtiohallinnon arkaluonteista dataa.

Arkaluontoisen julkisen datan käsittelyn vaatimuksia täydennettiin vuonna 2024 säädetyllä SREN-lailla ja vaatimukset vietiin käytäntöön huhtikuussa 2026 annetulla asetuksella. Elokuussa 2026 SecNumCloud 3.2 -vaatimustaso nostettiin arkaluontoisen julkisen datan käsittelyn viralliseksi kriteeristöksi.⁸

Vuonna 2025 Ranskan senaatin tutkintavaliokunta tarkasteli julkisia hankintoja ja niiden vaikutuksia Ranskan talouteen laajemmin. Digitaalisten hankintojen yhteydessä valiokunta kuuli muun muassa Microsoft Francen tuolloista lakiasiainjohtajaa **Anton Carniaux’ta** julkishallinnon pilvi- ja ohjelmistopalveluihin sekä niiden myötä rakentuviin riippuvuussuhteisiin liittyen. Kuuleminen osoitti hyvin, miksi digitaalista suvereniteettia pidetään tärkeänä. Carniaux’lta kysyttiin valan alla, voiko hän taata, etteivät Microsoftin hallussa olevat ranskalaisten tiedot päädy koskaan ulkomaiselle viranomaiselle ilman Ranskan viranomaisten suostumusta.

Vastaus oli: ”Non, je ne peux pas le garantir.” En voi taata sitä.⁹

Kyse ei ole Microsoftin moraalista, vaan lainsäädännöstä. Microsoft on yhdysvaltalainen yhtiö, joka toimii viime kädessä Yhdysvaltojen lain piirissä. Paljon puhutun CLOUD Actin myötä yhdysvaltalainen yhtiö voidaan pakottaa luovuttamaan käyttäjädataansa valtiolle riippumatta siitä, missä maassa sijaitsevalle palvelimelle data on varastoitu.

Sama periaate koskee muitakin suurvaltoja. Siksi digitaalista turvallisuutta ei voi rakentaa oletukselle siitä, että vieraan valtion lainsäädäntö pysyy aina meille suotuisana.

Suomen vastaus ovat tiekartta ja linjaus

Suomessa hallituksen ministerityöryhmä hyväksyi huhtikuussa 2026 digitaalisen suvereniteetin tiekartan. Siinä digitaalinen suvereniteetti määritellään kyvyksi hallita infrastruktuuria, dataa ja teknologioita ilman kohtuutonta riippuvuutta EU:n ulkopuolisista toimijoista. Painopisteiksi nimettiin kriittisten riippuvuuksien tunnistaminen, eurooppalaisten vaihtoehtojen kartoittaminen ja palveluiden jatkuvuuden turvaaminen.¹⁰

Kesäkuussa 2026 hallitus linjasi kansallisen tekoälyalustan ja laskentakapasiteetin rakentamisesta digitaalisen suvereniteetin vahvistamiseksi. Linjaus on erityisen ajankohtainen kansainvälisten datakeskustoimijoiden saapuessa joukolla Suomeen edullisen sähköön perässä.

Suurin alaan liittyvä uutinen tuli julki syyskuussa 2026, kun Google ilmoitti vähintään 13 miljardin euron investoinneista Suomeen vuosina 2027–2028. Investoinnit kohdistuvat digitaaliseen infrastruktuuriin ja sitä tukeviin hankkeisiin Haminaassa, Kajaanissa, Muhoksella ja Vaalassa.

Investointi on Suomelle merkittävä, mutta se ei poista kysymystä teknologisista riippuvuuksistamme.³

Kuten Carniaux’n valaehtoinen kuuleminen osoittaa, palvelimen sijainti Suomessa ei tee datakeskus-palvelusta juridisesti suomalaista. Esimerkiksi Yhdysvaltain lainsäädäntö ulottuu yhdysvaltalaisen palveluntarjoajan hallinnassa olevaan dataan myös silloin, kun data sijaitsee Euroopassa.

Tämän lisäksi datakeskuksiin liittyy kysymys sähköstä. Jos kaikki nyt suunnitellut hankkeet toteutuisivat täydessä laajuudessaan, Suomen sähkönkulutus kasvaisi lähes 40 prosenttia vuoden 2025 tasosta.⁶

F-Securen perustaja ja entinen toimitusjohtaja Risto Siilasmaa on nostanut esiin verkkouutisen aiheessa kansantalouden näkökulman. Hänen mukaansa Suomessa ei tarkastella datakeskusinvestointeja riittävästi kokonaisuutena: paljonko sähköä ne sitovat, paljonko pysyvää työtä ne synnyttävät ja mitä vaihtoehtoisia investointeja sama sähkö voisi mahdollistaa.⁴

Datakeskuksissa on kyse eri mittakaavan investoinneista kuin yritysten tai hankintayksikköjen teknologiavalinnoissa, mutta molempiin pätee sama periaate. Päätöksiä tehdään helposti nopealla tahdilla huomioimatta tarpeeksi niiden pitkän aikavälin vaikutuksia.

Digitaalinen riippuvuus näkyväksi hankinta-päätöksiin

Kesäkuussa voimaan tullut hankintalain uudistus olisi tarjonnut yhden tilaisuuden viedä digitaalisen suvereniteetin vahvistamisen käytännön hankintoihin. Uudistuksen tavoitteena oli ennen kaikkea lisätä kilpailua: suurempia hankintoja pitää jakaa osiin, yhden tarjouksen kilpailutuksia joudutaan tietyissä tilanteissa uusimaan ja sidosyksiköiden käytölle asetettiin vähintään kymmenen prosentin omistusvaatimus. Digitaaliin riippuvuuksiin uudistus ei kuitenkaan tarttunut.¹¹

Tässä näkyy Suomen ja Ranskan ero. Molemmissa maissa puhu-

taan digitaalisesta suvereniteetista. Ranska on muuttamassa sitä velvoitteiksi. Suomessa se on vasta tiekartta.

Ratkaisu ei ole eristäytyminen, eikä yhdysvaltalaisten palvelujen kieltäminen, vaan paljon arkisempi: mahdolliset riippuvuudet pitää tehdä näkyväksi ennen hankintapäätöstä.

Kriittiseen julkiseen digihankintaan pitäisi kuulua järjestelmällinen riippuvuusarviointi, jossa arvioidaan ainakin tekninen irtautumiskyky, irtautumisen kustannus ja aika, datan siirrettävyys, avoimet rajapinnat, oikeudellinen riippuvuus sekä palvelun jatkuvuus poikkeustilanteissa. Arvioitavat seikat pitäisi nostaa tarjousvertailun kriteereiksi hinnan ja toiminnallisuuden rinnalla.

”Emme voi vaihtaa, koska se maksaisi liikaa” ei ole luonnonlaki. Se on seuraus siitä, ettei mahdollisen vaihtamisen hintaa koskaan edes neuvoteltu. Siksi vielä tärkeämpää on sopia irtautumisen mahdollisuudesta silloin, kun toimittaja haluaa asiakkaan, ei vasta silloin, kun asiakas haluaa toimittajasta eroon. Sopimuksessa pitää määritellä datan vienti,

formaatit, dokumentaatio, rajapinnat, migraatiotuki, kustannukset ja määräajat.

Yhteishankinnoissa esimerkiksi Hansel voisi ottaa riippuvuus- ja irtautumiskriteerejä järjestelmällisesti käyttöön. Seuraavassa hankintalain uudistuksessa voidaan mennä pidemmälle ja tehdä riippuvuusarviointista velvoite ainakin merkittävissä ja yhteiskunnan toiminnan kannalta kriittisissä digihankinnoissa.

Tämä ei tarkoita, että suomalainen tai eurooppalainen toimittaja pitäisi valita hinnalla millä hyvänsä, vaan että tekniselle riippuvuudelle annetaan hinta.

Riippuvuus minkä tahansa yksittäisen ulkoavallan hyvästä tahdosta on rakenteellinen heikkous riippumatta siitä, kuka kyseistä valtiota sillä hetkellä johtaa. Hallitukset vaihtuvat. Lait muuttuvat. Pakotteita asetetaan. Teknologiaa käytetään vallan välineenä.

Riskiä ei voida poistaa valitsemalla suurvalloista oikea, vaan se poistetaan olematta täysin yhdenkään suurvallan armoilla.

LÄHTEET

1. Kilpailu- ja kuluttajavirasto, “KKV antoi VR:lle huomautuksen laittomasta IT-palveluiden suorahankinnasta”, 12.6.2025; päätös 4.3.2025. kkv.fi.
2. Kilpailu- ja kuluttajaviraston päätös R/2024/60, 4.3.2025. kkv.fi/uploads/sites/2/r-2024-60-0024.pdf.
3. Google, “Google Deepens Commitment to Finland with Two-Year EUR13 Billion investment in AI Infrastructure”, 9.9.2026. googlecloudpresscorner.com.
4. Risto Siilasmaan datakeskuksia koskevat arviot, ks. Verkkouutiset, “Risto Siilasmaa HS:lle: Datakeskukset vievät sähköön, hyöty jää vähäiseksi”, 2026. verkkouutiset.fi.
5. Euroopan komissio, ehdotus Cloud and AI Development Act -säädöksi, COM(2026) 502. eur-lex.europa.eu.
6. Euroopan komissio, “Strengthening Europe’s tech sovereignty”, 3.6.2026. commission.europa.eu.
7. Euroopan komission tiedotustilaisuus 3.6.2026; varapuheenjohtaja Henna Virkkusen kommentit teknologiasuvereniteetista ja kriittisten palvelujen “kill switch” -riskistä. audiovisual.ec.europa.eu.
8. Ranska: Cloud au centre -doktriini; SREN-laki (2024), 31 artikla; décret n° 2026-272, 14.4.2026; SecNumCloud 3.2 -vaatimusten vahvistaminen elokuussa 2026. legifrance.gouv.fr.
9. Ranskan senaatin tutkintakomission kuuleminen 10.6.2025; Microsoft Francen lakiasiainjohtaja Anton Carniaux. senat.fr.
10. Valtioneuvosto, “Ministerityöryhmä linjasi digitaalisen suvereniteetin vahvistamisesta - tiekartta ohjaa toimia hallituskauden loppuun”, 27.4.2026. valtioneuvosto.fi.
11. Valtioneuvosto, “Uusi hankintalaki voimaan - lisää kilpailua julkisiin hankintoihin”, 2026. valtioneuvosto.fi.

KIRJOITTAJA:



Repe Harmanen toimii Netum Group Oyj:n toimitusjohtajana. Netum on suomalainen IT-palvelutalo, joka auttaa julkista sektoria ja yrityksiä rakentamaan toimivampaa ja turvallisempaa digiyhteiskuntaa. Cyberwatch Finland liittyi osaksi Netumia keväällä 2026.

REPE HARMANEN

Toimitusjohtaja
Netum Group Oyj



➤ RISTO RAJALA
& PETER SUND

Kyberturvallisuuden rahoitus ja yritysten toimintaympäristö ratkaisevat Suomen turvallisuuden

Poliittiset päättäjät, virkamiehet ja yhteiskunnalliset toimijat valmistautuvat keväällä 2027 järjestettävään Eduskuntavaaleihin. Vaalien keskeisimmäksi teemaksi näyttää jälleen nousevan julkisten varojen käyttö, sillä valtion velkaantumista ei ole saatu taistamaan istuvan hal-

lituksen kunnianhimoisista tavoitteista huolimatta. Samaan aikaan heikentyneen turvallisuustilanteen ja NATO:oon liittyvien sitoumusten vuoksi puolustusmenoja joudutaan kasvattamaan, minkä vuoksi yhteiskunnan muihin sektoreihin kohdistuvat sopeutustarpeet korostuvat

entisestään. Valtavat säästöpainee-
t tulevat väkisin määrittämään
tulevia hallitusohjelmaneuvoitteluita,
varsinkin kun lähes kaikki eduskun-
tapuolueet kahta lukuun ottamatta
ovat sitoutuneet parlamentaarisesti
sovittuun velkajarruun, jossa ne ovat
määritelleet yhteisesti sopeutustar-

peen tason, jättäen kuitenkin keinot poliittisessa päätöksenteossa määritettäväksi.

Julkisen talouden vaikea tilanne heijastuu suoraan myös kyberturvallisuuden kehittämiseen. Digitalisaation myötä lisääntyvä hyökkäyspinta-ala, tekoälytyökalujen entisestään kiihtyvä hyödyntäminen kyberrikollisuudessa ja valtiollisten toimijoiden kasvava halukkuus hyödyntää tietojärjestelmiä vakoiluun ja sabotaasiin asettavat yritykset ja organisaatiot valtavan haasteen eteen digitaalisten riskiensä hallinnassa – pahaa tahtoa siis riittää. Samaan aikaan haavoittuvuuden taso on liian korkea: olemme arvioineet, että kyberturvallisuuslain soveltamisalaan kuuluvilla toimialoilla, kuten vesihuollossa ja energia-alalla, on kullakin noin 100-150 miljoonan euron investointivaje uhkia vastaavan tason saavuttamiseen, mikä tarkoittaa kokonaisuudessaan jopa kahta miljardia euroa.

Kyberturvallisuus on turvallisuuden ydinaluetta sisäisen turvallisuuden sekä sotilaallisen maanpuolustuksen ohella. Tieto- ja viestintäjärjestelmien toimintavarmuus sekä tiedon luottamuksellisuus ja eheys ovat osa kokonaisturvallisuutta, yhteiskunnan päivittäistä toimintakykyä, yritysvaarallisuuden ja elinkeinotoiminnan taloudellisten edellytysten, teollisen tuotannon sekä huoltovarmuuden turvaamista. Kyse on keskeisestä osasta talouden rakenteita, yritysten prosesseja, tuotantoyrityksiä ja datan omistajuutta. Yritykset ja yhteisöt ovat kyberturvallisuuden etulinja, sillä ne omistavat järjestelmät, tunnistavat poikkeamat ja toteuttavat käytännön suojaustoimet ja vastaavat niistä koskevista häiriöistä palautumisesta. ICT-ratkaisuiden toimintavarmuuteen ja kyberturvallisuuteen liittyvät kysymykset ovat osa jokaisen organisaation riskienhallintaa. Julkisen talouden vaikeuksista huolimatta, ja osin myös niiden vuoksi, on välttämätöntä, että valtio tarjoaa taloudellisia kannustimia yhteiskunnan kriittisillä sektoreilla

toimiville yrityksille ja kyberturvallisuuden kumppaneista riippuville pk-yrityksille kyberturvallisuusriskien hallitsemiseksi. Kannustimien avulla korjattaisiin selkeitä markkinapuitteita, vahvistettaisiin kansallista turvallisuutta laajasti ja tuettaisiin parempien teknologioiden käyttöönottoa. Toiminta loisi kysyntää kotimaisille teknologia- ja turvallisuusratkaisujen tarjoajille. Olemmekin esittäneet, että panostukset puolustuksen ja turvallisuuden vahvistamiseksi tehtäisiin poikkeuksellisesti eri ministeriöiden välillä tunnistettuja tarpeita priorisoiden.

Kansalaismielipide tukee ehdottamiamme tavoitteita; komission tuoreen Eurobarometrin mukaan 96 % suomalaisista katsoo, että EU:n ja jäsenmaiden on vahvistettava kyberturvallisuutta – enemmän kuin minkään muun digipolitiikan tavoitteen kohdalla – ja 98 % pitää tietoturvan ja yksityisyyden suojaamista verkossa tärkeänä. Suvereniteetin suhteen 93 % priorisoi investoinnit Euroopassa kehitettyyn ja hallinto- ja digitaaliseen infrastruktuuriin – ja mikäli palveluntarjoajaa vaihdettaisiin, tärkein vaihtamisen syy on turvallisuus ja luotettavuus. Kriittisten sektorien investointivajeen kattamiselle, parempien ratkaisujen hyödyntämiselle julkisissa hankinnoissa ja kyberturvallisuuden viennin edellytysten rakentamiselle on siis poikkeuksellisen vahva kansalais-tuki.

Julkisten varojen käytön ja EU-säätelyn lisäksi käynnissä on myös kansallisia lainsäädäntöprosesseja, joilla on toteutuessaan merkittäviä vaikutuksia yhteiskunnan kyberturvallisuuteen sekä kyberturvallisuusteollisuuden toimintaedellytyksiin. Kotimaan politiikassa olemme keskittyneet kuluneen vuoden aikana erityisesti hankinta- ja vientisääntelyn, ”tietoturvallisuuden arviointilain”, pilvipalveluiden turvallisuuteen ja tiedustelulakien uudistamiseen. Alla käsitellään tarkemmin arviointilakia sekä sotilas-tiedustelulakia.

Yrityksille lisää liiketoimintamahdollisuuksia tietojärjestelmien arvioinneista

Hallitus antoi vuonna 2026 lakiehdotuksen ”arviointilaki”, jolla muutettaisiin viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden ja varautumisen arviointia koskevaa lainsäädäntöä. Kokonaisuudistus on kannatettava ja se vahvistaa julkishallinnon kriisinkäsittelevyyttä, selkeyttää viranomaisten vastuuta ja parantaa arviointien saatavuutta. Lakiuudistuksen myötä viranomaiset voivat käyttää yksityisiä asiantuntijoita ja yrityksiä laajemmin arviointien tukena.

On tärkeää, että turvallisuuskriittisten ratkaisujen ja niitä valmistavien yritysten arviointi ja hyväksyntä säädetään lakiin. Tämä lisää läpinäkyvyyttä, yhdenmukaistaa kansalliset menettelyt EU- ja NATO-vaatimusten kanssa sekä parantaa kotimaisten toimijoiden kilpailukykyä. Muutos selkeyttää yritysten toimintaympäristöä ja vahvistaa luottamusta suomalaisiin turvallisuusteknologioihin. Laissa säädetään arviointivelvollisuudesta valtionhallinnon viranomaisille. Velvollisuus toteuttaa vähintään itsearviointi ja tietyissä turvallisuusluokissa riippumaton arviointi parantaa riskienhallintaa ja yhtenäistää tulkintoja. Velvoite selkeyttää vastuunjakoja ja tukee viranomaisten tietojärjestelmien turvallista käyttöönottoa ja ylläpitoa, ja siten yhteiskunnan kyberturvallisuuden tasoa kokonaisuutena. Lakiesityksessä ehdotetaan Puolustusvoimille arviointiviranomaisen roolia, mikä on perusteltua kasvaneisiin arviointitarpeisiin liittyen. Jatkovalmistelussa tulisi kuitenkin huolellisesti varmistua siitä, että arviointitehtävä säilyy kaikilta osin rajallisena, täsmällisenä ja koskettaa ainoastaan välttämätöntä osaa Puolustusvoimien toiminnasta ja järjestelmistä.

Lakiuudistuksessa arviointimenettelyjä myös laajennetaan ja täsmennetään. Arviointien sujuvoit-

tamiseksi ja saatavuuden parantamiseksi sekä sääntelyn selkeyttämiseksi arviointilakiin sisältyy viranomaisen toteuttama itsearviointi ja viranomaisen toimeksiannosta palveluntarjoajan toteuttama arviointi. Viranomaisen toimeksiannosta toimiva palveluntarjoaja voisi arvioida tietojärjestelmiä, joissa käsitellään julkisia, salassa pidettäviä ja korkeintaan turvallisuusluokkaan IV luokiteltuja tietoja. Erityisesti mahdollisuus käyttää palveluntarjoajan toteuttamaa arviointia parantaa arviointien saatavuutta, vähentää ruuhkautumista ja tukee asiaa koskevan elinkeinotoiminnan edellytysten ylläpitoa ja kehittämistä. Menetelyjen selkiyttäminen lisää kustannustehokkuutta, viranomaisten toimintavarmuutta ja arviointimenettelyn päämäärien saavuttamista tavoiteaikataulussa.

On myönteistä, että arviointilaitosten pätevyyksien hyväksy-

mismenettelyjä joustavoitetaan ja selkeytetään. Muutos tukee arviointipalveluiden riittävää tarjontaa ja lisää markkinoiden toimivuutta. Esimerkiksi hajasäteilyyn liittyviä ratkaisuja tarjoavien TEMPEST-yritysten mahdollisuus hakea hyväksyttyä asemaa on kannatettavaa. Tietoturvallisuuden arviointilaitoksena toimivan yrityksen luotettavuuden varmistamista yksinkertaistettaisiin ja tehostettaisiin säätämällä yritysturvallisuus selvityksen tekemisestä, jos tietoturvallisuuden arviointilaitos hakee pätevyyttä turvallisuusluokitellun tiedon käsittelyn arviointiin. Yritysturvallisuus selvitysten käyttö oikeissa kohdissa vahvistaa luotettavuutta. Samalla on olennaista, että Suojelupoliisi ottaa huolellisesti tehtävään liittyvän muutoksen huomioon toimintansa suunnittelussa ja ohjauksessa. Yritysturvallisuus selvitysmenettelystä ei muodostu tosiasiallista pullonkaulaa toiminnalle.

Esimerkkinä sotilas-tiedustelulain muutosten vaikutukset yrityksiin

Hallituksen esitys sotilastiedustelulain muuttamisesta on ollut käsitteilyssä Eduskunnassa syksyllä 2026. Lakiehdotus tähtää Puolustusvoimien tiedustelutoiminnan tehostamiseen ja kansallisen turvallisuuden turvaamiseen nykyaikaisin toimivaltuuksin. Esityksen tavoite on hyväksyttävä, koska sotilastiedustelun toimivaltuuksien on vastattava turvallisuusympäristöä ja teknologian kehitystä. Se kohdistuu kuitenkin poikkeuksellisen suoraan yrityksiin, kuten datakeskuksiin, viestinnän välittäjiin, laite- ja ohjelmistovalmistajiin sekä yrityksiin, joiden järjestelmiä voitaisiin käyttää myös tiedustelun välineenä.

Lakiehdotuksen jatkovalmistelussa on korjattu useita elinkeino-

elämän aiemmin esille nostamia puutteita. Esityksen perusteluissa todetaan nyt, ettei yrityksiä velvoiteta purkamaan päästä päähän -salausta tai asentamaan takaportteja ja että salausta on välttämätön Suomen kokonaisturvallisuudelle. On myös olennaista, että tietoliikennetiedustelun hakuehtoja tarkennetaan, ja että avustamisvelvollisuus rajataan kyberturvallisuuslain mukaisiin datakeskuspalvelun tarjoajiin. Myös esitykseen tehdyt tarkennukset kotimaassa valtiollisen toimijan tietojärjestelmään kohdistuvan tiedustelun lupamenettelyyn ovat tarpeellisia.

Lakiuudistuksen keskeisin avoin kysymys koskee yritysten asemaa tiedustelutoimenpiteen kohteena. Jos yritys havaitsee järjestelmässään sotilastiedustelun asentaman ohjelmiston tai vieraan laitteen, kyse on tietoturvapoikkeamasta, josta voi seurata kyberturvallisuuslain mukainen ilmoitusvelvollisuus. Yritys voisi siis joutua tutkimaan, raportoimaan ja korjaamaan valtion omaa toimenpidettä ja kantamaan kustannukset ja maineriskin. On oltava selvää, ettei tällainen poikkeama voi johtaa seuraamuksiin yritykselle tai sen johdolle. Muun kuin valtiollisen toimijan tietoliikennetiedustelusta tulisi ilmoittaa Suomessa laillisesti oleskelevalle henkilölle ja laillisesti toimivalle yritykselle, sillä Perustuslakivaliokunnan mukaan ilmoitusvelvollisuus voisi turvata oikeusturvaa paremmin.

Lakiesitys käsittelee myös Suomen ulkopuolella oleviin tietojärjestelmiin kohdistuvia toimenpiteitä. Olemme katsoineet, että niistä tulisi päättää valtion poliittisen johdon tasolla ja menetelmien käyttö tulee rajata vakavan ja välittömän uhan torjuntaan. Näin siksi, että mahdolliset vastatoimet kohdistuisivat todennäköisesti yritysten hallussa olevaan kriittiseen infrastruktuuriin ja yritysten liiketoimintamahdollisuuksiin. Yrityksen työntekijän osallistuminen tiedustelun avustamiseen edellyttäisi lisäksi työnantajan tietoa ja suostumusta. Tiedustelulainsä-

dännön muutosten yhteisvaikutuksia on myös hyvä arvioida kokonaisuuksena, sillä lakiuudistuksen yhteydessä käsitellään myös tulevaa asumistiloja koskevaa esitystä, joka sallisi tiedusteluvaltuuksien käytön kodeissa – jotka siis ovat myös etätyötoimistoja. Olemme myös edellyttäneet, että peitteen käytön rajat ja valvonta avointen lähteiden tiedonhankinnassa kirjataan lakiin. Yksityiseltä yhteisöltä saatavien tietojen ei pidä mahdollistaa salaisten tiedonhankintakeinojen edellytysten kiertämistä. Tarkkarajainen ja valvottava sääntely vahvistaa luottamusta Suomeen turvallisenä ja ennakoitavana toimintaympäristönä, mikä on tärkeää ei vain kyberturvallisuusyritysten sijaintimaana, mutta myös Suomen asemalle datakeskusten ja tietoliikenne-infran solmukohtana.

Kohti Eduskuntavaaleja

Menestyvä, kasvava ja kansainvälistyvä kyberturvallisuusteollisuus on monella tapaa maamme turvallisuuden ja hyvinvoinnin, sekä yhteiskuntamme toimintojen yllä-

pitämisen elinehto. On keskeistä, että tuleva hallitus, oli se sitten millainen tahansa, kykenee löytämään tarvittavat resurssit kyberturvallisuuden ylläpitämiseen ja kehittämiseen elinkeinoelämän toimintaedellytykset varmistaen. Samalla on varmistettava, ettei lainsäädännöllisissä tai hallinnollisissa prosesseissa anneta viranomaisille toimivaltuuksia, jotka heikentäisivät markkinoilla toimivien yritysten liiketoimintamahdollisuuksia tai vaarantaisivat omaisuuden sekä yksityisyyden ja luottamuksellisen viestinnän perusoikeussuojaa. Viestinnän luottamuksellisuuden ja toimivien markkinoiden takaaminen ja vahvistaminen ovat elinehto kotimaiselle kyberturvallisuusteollisuudelle ja laajemmin maamme digitaaliselle taloudelle.

Kyberalan vaikuttamistyö jatkuu aktiivisena. Pidämme esillä kyberturvallisuusteollisuuden ja yhteiskunnan kyberturvallisuuden kannalta olennaisia asioita niin julkisessa keskustelussa, kuin tapaamisissa poliittisten päättäjien, virkamiesten ja muiden sidosryhmien kanssa.

KIRJOITTAJAT:



PETER SUND

Kyberala ry:n (FISC ry)
toimitusjohtaja
Teknologiateollisuus ry



RISTO RAJALA

Kyberala ry:n (FISC ry)
neuvonantaja
Teknologiateollisuus ry



Datamyrkytys ja RAG-myrkytys

Artikkeli perustuu muistioon ja siitä tehtyyn esitykseen, esitetty King's College Londonissa kesällä 2026.

Datamyrkytys on jaetun datan **ehyteen eli oikeellisuuteen kohdistuva hyökkäys**: hyökkääjä ei varasta tietoa vaan turmelee sen, jolloin jokainen tällä datalla koulutettu malli tai siitä tietoa hakeva järjestelmä perii hyökkääjän tavoitteet. Uhka koskettaa erityisesti avointa ja yhteistyöhön perustuvaa tutkimusta, jonka arvo perustuu luottamukseen datan, jota ei ole itse tuotettu, eheydestä. Tarvittava datan myrkytyksen määrä on pientä ja sen toteutus on halpaa:

Noin **0,001 %:n koulutustokeneista** korvaaminen riitti turmelemaan lääketieteellisen kielimallin (Large Language Model, LLM) vastaukset [2]. Tarvittavien myrkytettyjen dokumenttien määrä on **lähes vakio – noin 250 – mallin koosta riippumatta** [24], ja hakuavusteisessa generoinnissa (Retrieval-Augmented Generation, RAG) jo viisi syötettyä dokumenttia saavutti 90 %:n onnistumisasteen miljoonan dokumentin tietovarastoa vastaan [13]. Kolmas päivitys (lokakuu 2026) lisää koosteen ja ”tietopäivitys”-myrkytyksen [39–44], kysymys–vastaus-käytön ulkopuolelle ulottuvan myrkytyksen ja agenttien muistin myrkytyksen [45–49, 54], ensimmäinen todis-

tetusti kestävä aggregointipuolustus [53] sekä EU:n Digital Omnibus -asetuksen [59].

1. Myrkytys jaetun datan eheyttä uhkaavana tekijänä

Toisin kuin luottamuksellisuuden loukkaukset, myrkytys kohdistuu datan ja sitä käyttävien mallien luotettavuuteen. Se on **huomaamaton** (kokonaismittarit voivat näyttää hyviltä, vaikka kapea toiminto on turmeltunut), **halpa** (pieni myrkytetty osuus riittää) ja **pysyvä** (se säilyy mallin painoissa tai tietopohjassa, kunnes se havaitaan).

Ne avoimen tieteen kanavat, jotka tekevät datasta arvokasta, muodostavat myös hyökkäyspinnan: joukkoistetut aineistot, julkiset repositoriot ja toimitusketju, kaavitut esikoulutusaineistot, federoitu oppiminen ja jopa vertaisarviointi. Kun yhdelle suositulle käyttäjäsivulle lisättiin vain 13 sanaa, hyökkääjän teksti päätyi lähteeksi 38–51 %:iin syvätutkimusagenttien raporteista [46].

BadRAG sai noin 0,04 % korpuksesta haetuksi 98,2 %:n onnistumisasteella ja nosti GPT-4-pohjaisen RAG:n kieltäytymisasteen 0,01 %:sta 74,6 %:iin [15]. Noin 250 dokumentin raja piti malleissa 600 miljoonasta

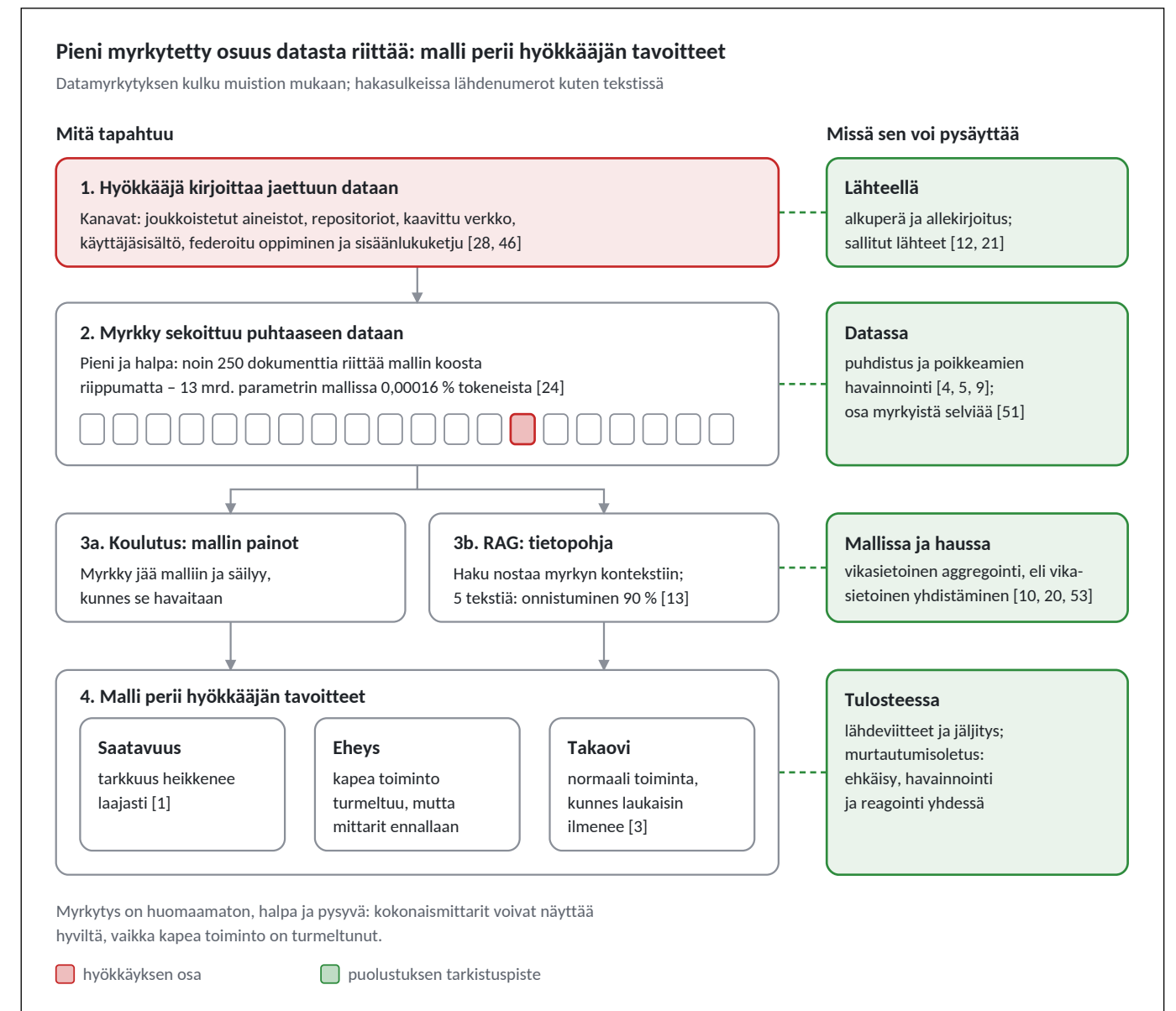
13 miljardiin parametriin – suurimmassa vain 0,00016 % tokeneista – mikä kumosi oletuksen, että suuremmat mallit vaatisivat suhteessa enemmän myrkytystä [24].

2. Uhkamaisema: perinteinen datamyrkytys

Hyökkäysten tavoitteet jakautuvat kolmeen. **Saatavuus** (kohdentamaton) heikentää tarkkuutta laajasti [1]; **eheys** (kohdennettu) turmelee toiminnan kapealla osa-alueella jättäen kokonaismittarit ennalleen; ja **takaovi** upottaa harvinaisen laukai-

simen, jolloin malli toimii normaalisti, kunnes laukaisin ilmenee, ja tavalliset testiaineistot pysyvät puhtaina [3].

Menetelmät vaihtelevat **luokkien vaihtamisesta puhdasluokkaiseen** ja optimointipohjaisiin myrkytyksiin; pienten myrkytettyjen datojen osuuksien ja suurten vaikutusten epäsuhta on keskeinen riski [2, 24]. Vuoden 2026 tulokset nostavat rimaa: pelkkä myrkkijoukon valinta muutti takaoven onnistumisasteen 3 %:sta 80 %:iin [50], Phantom Transfer selviää yhdestätoista datatason puolustuksesta [51], ja takaovista on tulossa ohjelmoitavia [57] – satun-



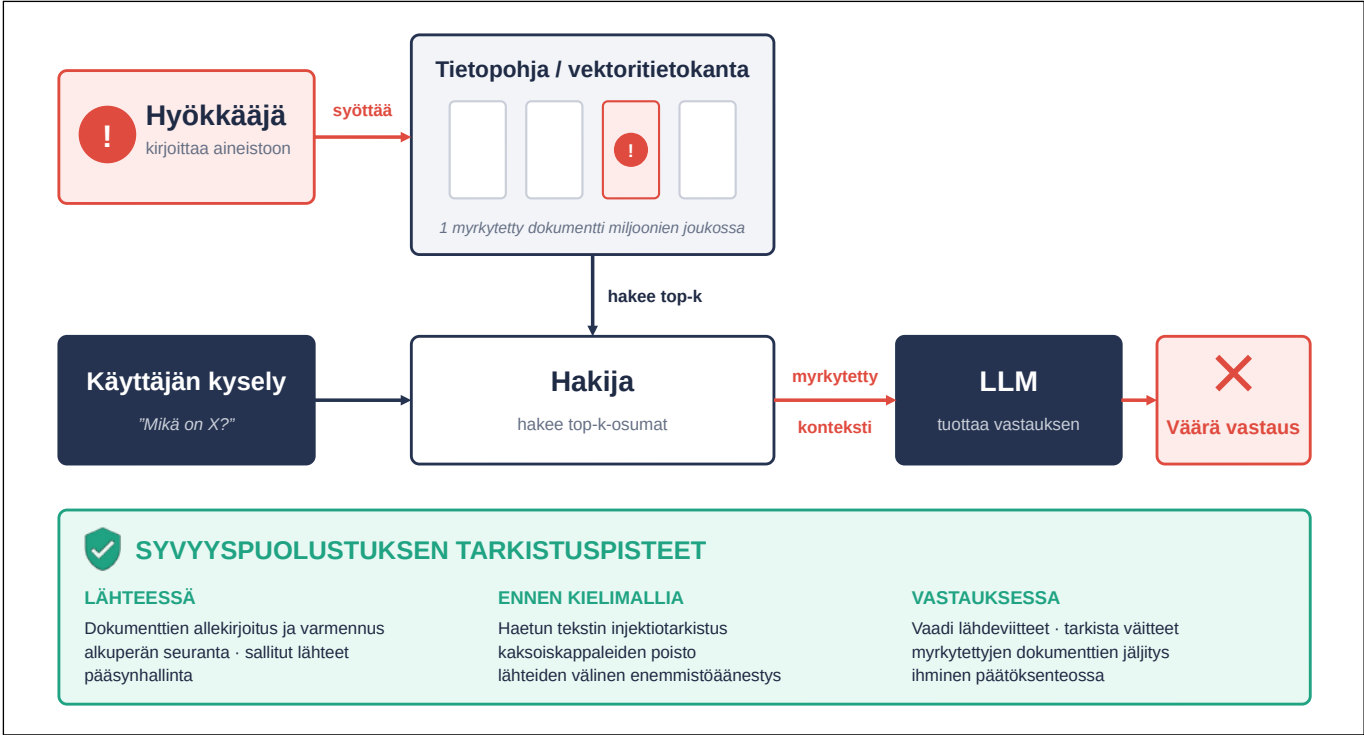
Kuva 1. Datamyrkytyksen kulku sisääntulosta vaikutuksiin ja monikerroksisen puolustuksen tarkistuspisteet.

naisotantaan perustuvat arviot ali-arvioivat pahimman tapauksen. Myrkytyksen sisään tuloreittejä ovat datan keruu, kuratointi, pake-tointi ja jakelu, jatkuva päivittäminen, sisäänlukutyökaluketju [28] sekä hajautettu hienosäätö, jossa yksi solmu voi istuttaa takaoven vertaisiinsa [55].

3. RAG-myrkytys: tieto-pohja hyökkäyspintana

Hakuavusteisen generoinnin tietopohja on uusi ja käytännöllinen hyök-käyspinta: hyökkääjä, jolla on suora tai epäsuora kirjoitusoikeus, voi syöttää dokumentteja, jotka hakumalli nostaa

esiin ja joihin malli luottaa [13]. Myr-kytetyn dokumentin on oltava **haet-tavissa ja ohjaava** – se sisältää vää-rän vastauksen tai **epäsuoran keho-teinjektion**. Kohteet ulottuvat nyt agenttien muistiin, koodingeneroin-tiin [45], tietoturvatyökaluihin [54] ja syvätutkimusagentteihin [46, 47].



Kuva 2. RAG-myrkytyksen kulku ja monikerroksisen puolustuksen tarkistuspisteet.

4. RAG-hyökkäysten taksonomia

Hyökkäykset voidaan luokitella viiden toisistaan riippumatto-man ulottuvuuden mukaan: **put-ken vaihe** (haku tai generointi [15]), **pääsy** (musta tai valkoinen laatikko, vahvimpana hakumallin hienosäätö), **kyselyriippuvuus, laa-timistapa** (heuristinen, optimoin-tipohjainen [14] tai koosteinen [39, 40]) ja **tavoite** (kohdennettu vastaus, palvelunesto, ohjaus, turvarajoitus-ten ohitus, datavuoto tai turvaton koodi [45]).

5. Uhka-hallinta-keino-matriisi

Matriisi yhdistää kunkin uhan havainnointi-, ennaltaehkäisy- ja reagoitikeinoihin. Mikään yksit-täinen keino ei riitä; tavoitteena on kerroksellinen kattavuus. Alkupe-räisen 18 uhkaa on tässä ryhmitelty seitsemäksi.

6. Havainnointimenetelmät

Koulutusdatalle: spektrisignatuurit [4], aktivaatioklusterointi [5], vaiku-tusfunktioihin perustuva attribuutio [9], laukaisimen takaisinmallinnus

[6], STRIP [7], fine-pruning [8] sekä kanarialintuesimerkit, jotka mallin pitäisi oppia odotetusti. **RAG:lle:** haku- ja upotuspoikkeamat, tekstiosien tarkastus kehotein-jektion varalta, lähteiden välinen johdonmukaisuus ja jäljitys virheel-lisestä vastauksesta vastuussa oleviin dokumentteihin. Myrkytetyillä vas-tauksilla voi olla pienempi perplek-siteetti kuin harmittomilla, mutta huomio ”romahtaa” myrkytettyihin dokumentteihin, minkä D-SCAN havaitsee silloinkin, kun vastaus ei muutu [52]; luottamuksen pehmeä alentaminen toimii paremmin kuin jyrkkä suodatus [54].

HYÖKKÄYS	VAIHE; PÄÄSY	PÄÄTAVOITE
PoisonedRAG [13], CorruptRAG [31], Confundo [30]	Haku + generointi; musta laatikko	Kohdennettu, koko käsittelyputken kestävä vastaus
BadRAG / TrojRAG [15]	Hakuvaiheen takaovi; valkoinen laatikko	Palvelunesto / semanttinen ohjaus
HijackRAG [17]	Generointi; musta laatikko	Vastauksen kaappaus
Korpuksen myrkytys [14], MIRAGE [29], POISONCRAFT [19]	Haku; kyselystä riippumaton	Haun saastuttaminen / väärä tieto
Poisoned-MRAG [18] / One Pic [28]	Multimodaalinen; optimoitu kuva	Kohdennettu vastaus / disinformaatio
GRAGPoison [28], KG-RAG / KEPo / LogicPoison [32–34]	GraphRAG; graafirakenteen huomioiva	Päätteilypolun kaappaus
DisarmRAG [35]	Hakumallin muokkaus; valkoinen laatikko	Itsekorjauksen tukahduttaminen
InceptionRAG [39], mikroyhteistoiminnallinen [40]	Koosteinen; useita katkelmia / lähteitä	Johdateltu väärä päätelmä
ToxicRAG / PURPOSE / DenialRAG / RAG-NAROK [41–44]	Ristiriitojen ratkaisu; yksi dokumentti	Ristiriitapuolustusten kiertäminen
CodePoisonRAG [45]	Kooditietopohja; ≤1 artefakti	Turvaton koodi (CWE)
Käyttäjäsältö / verkkonäyttö [46, 47]	Reaaliaikainen verkkohaku	Raporttien manipulointi
AgentPoison [16], GhostWriter [48]	Agentin muisti; laukaisin / piilotettu hyötykuorma	Pysyvä haitallinen toiminto

Taulukko 1. Edustavat RAG-myrkytyshyökkäykset taksonomiaulottuvuuksittain (tiivistetty).

UHKA	HAVAINNOINTI	ENNALTAEHKÄISY	REAGOINTI
Koulutusdatan myrkytys (saatavuus, eheys, takaovi)	Alaryhmäseuranta; vaikutusfunktiot; spektrisignatuurit; STRIP	Alkuperätieto + allekirjoitus; kuratointi; myrkytystä sietävä ja häiriönsietoinen opetus/koulutus	Uudelleen koulutus; fine-pruning; poisoppiminen
Federoitu oppiminen ja hajautettu hienosäätö	Päivitysjakauman poikkeamat; adapterien seulonta	Vikasietoinen aggregointi, eli vikasietoinen yhdistäminen (Krum, työstetty keskiarvo); Chorus	Solmun poissulkeminen; uudelleenaggregointi
Toimitusketju ja sisäänluku	Tiiviste- ja allekirjoitusristiriidat; jäsenintarkastus	Allekirjoitetut artefaktit; BOM; luotetut lataimet	Karanteeni; palautus todennettuun versioon
RAG-tietopohja ja kehoteinjektio	Haku- ja upotuspoikkeamat; ohjekuvioiden tarkastus; jäljitys	Sallitut lähteet; haettu teksti epäluotettavana	Poisto; uudelleenindeksointi; vastaus useista lähteistä
Koosteinen, opittu ja ristiriitoja kiertävä myrkytys	Huomiopoikkeamat (D-SCAN, AV Filter); katkelmien johdonmukaisuus	Eistäminen (HODOR); PRA-RAG; auktoriteettiin perustuva järjestys	Katkelmaketjun jäljitys ja poisto; riippumaton uudelleentodennus
GraphRAG- ja kooditietopohjat	Topologia-poikkeamat; CWE- ja staattinen analyysi	Kolmikoiden alkuperätieto; allekirjoitetut kooditietopohjat	Kolmikoiden karsinta; koodin auditointi
Agentit: työkalut, muisti, verkkohaku, arviointi	Muistin eheystarkistukset; lainattujen lähteiden valvonta	Vähimmät oikeudet; allekirjoitettu muisti; käyttäjäsallön painon alentaminen	Muistin palautus; raporttien uudelleengenerointi; ihmisen arvio

Taulukko 2. Uhka-hallintakeino-matriisi (tiivistetty).

7. Puolustus ja lieventäminen (moni-kerroksinen puolustus)

- **Alkuperä ja eheys:** jäljitä alkuperä; allekirjoita data- ja mal-liartefaktit; versioi. Alkuperä-tieto mahdollistaa attribuution ja palautumisen [12, 21].
- **Lähteiden ja toimitusketjun hygienia:** suosi todennettuja lähteitä; vältä valikoimatonta datan kaavintaa; arvioi kolman-sien osapuolten aineistot ja mal-lit mallikorttien avulla.
- **Puhdistus ja häiriönsietoinen koulutus:** vikasetoinen aggre-gointi – Krum [10], typistetty keskiarvo / mediaani [11]. Cho-rus laski hajautetussa hienosäädössä hyökkäyksen onnistu-misasteen 48–63 %:sta enintään 2,2 %:iin [55], ja poisoppiminen poisti suurimman osan agent-tien takaovista [56]. Koska osa myrkyistä selviää kaikista data-tason suodattimista [51], tarvitaan myös koulutuksen jälkeiset mallien auditoinnit.
- **RAG-kohtaiset hallintakeinot:** sallitut lähteet; haettu teksti epä-luotettavana (upotettuja ohjeita ei koskaan suoriteta); haun jäl-keinen suodatus (FilterRAG) [25]; eristä-ja-aggregoi-gene-rointi (RobustRAG) [20]; harva dokumenttihuomio (SDAG) [27]; huomiopohjainen havain-nointi (AV Filter) [36]; tiedon-kulun hallinta (Cordon-MAS) [37]; allekirjoitettu agentti-muisti (SMSR) [38]; todistetusti kestävä aggregointi (PRA-RAG) [53]; dokumenttien eristäminen (HODOR) [39]; muistin haku-seulonta (AM-Sentry) [48]; ja syvätutkimusagenteilla riippu-vuuden rajaaminen yksittäisistä käyttäjäsisivuista – niiden täydel-linen poisjättäminen heikentää raporttien laatua [46].
- **Pääsynhallinta ja auditointi:** rajoita, kuka voi kirjoittaa aineis-toihin ja tietopohjiin; ylläpidä peukalointia paljastavia audi-tointilokeja.

8. Hallinto ja standardit

Ankkuroi ohjelma tunnustettuihin viitekehyksiin: **NIST AI 100-2** [21], **OWASP Top 10 for LLM Applica-tions** (LLM04:2025) [22] ja agenttien ASI06 Memory & Context Poisoning [58] sekä **EU:n tekoälysäädös**, joka tekee myrkytyksen kestävyydestä suuririskisten järjestelmien velvoit-teen (artiklat 10 ja 15) [23]. Digital Omnibus -asetus (EU) 2026/1744 siirtää nämä vaatimukset liitteen III järjestelmille 2.12.2027:ään ja tuotteisiin sulautetulle tekoälylle 2.8.2028:aan [59]. Velvoitteita on lykätty, ei poistettu, joten väliaika kannattaa käyttää alkuperä- ja vika-sietoisuusnäytön rakentamiseen.

9. Viimeaikainen kehitys (2025–2026)

2025. Merkittävin tulos on, että myrkytys vaatii **lähes vakiomää-rän dokumentteja** mallin koosta riippumatta [24]. RAG-hyökkäyk-set laajenivat kyselystä riippumat-tomiin, graafi-, multimodaalisiin ja sisäänlukuketjun hyökkäyksiin [18, 19, 28, 29], ja puolustukset haun ja generoinnin rajapintaan [20, 25, 27] – auttaen vain osittain [13, 18].

Tammi-kesäkuu 2026. Con-fundo osoitti, että oppimiseen perus-tuvat ”putkenkestävät” myrkyt ovat jopa noin 1,7-kertaisesti tehokkaam-pia myös puolustusten ollessa käytössä [30, 31]; jäsenNELTY RAG nousi ensisi-jaiseksi kohteeksi [32–34]; ja Disar-mRAG myrkyttää itse hakumallin, tukahduttaen kielimallin itsekorjauk-sen yli 90 %:n onnistumisasteella [35].

Heinä-lokakuu 2026. Myrkytyk-sestä tuli koosteista (InceptionRAG yli 80 % [39, 40]); yhden dokumen-tin hyökkäykset kiertävät ristiriitojen ratkaisun esiintymällä tietopäivityk-sinä (ToxicRAG 61–91 % [41–44]); CodePoisonRAG saavuttaa 0,7 %:n myrkytysosuudella 80–93 %:n onnis-tumisasteen [45]; ja agenttien muis-tiin syötetty haitallinen sisältö säilyi 84 %:ssa tapauksista [48, 49].

Puolustukset 2026. Huomiopoh-jaiset menetelmät palauttavat noin

20 % tarkkuudesta, mutta mukau-tuvat hyökkäykset onnistuvat yhä noin 35 %:ssa [36]. PRA-RAG las-kee onnistumisasteen jopa 1 %:iin 71 %:n tarkkuudella [53]. Jokaisen uuden hyökkäysperheen osoitettiin kuitenkin kiertävän osan olemassa olevista puo-lustuksista [39, 41–45] – edistysaskeleet ovat puolustuskohdaisia eivätkä yleisiä.

10. Jäännösriski ja avoimuuden jännite

Puolustukset ovat epätäydellisiä: tavanomaiset lievennyskeinot aut-tavat vain osittain [13, 18], havait-simet ovat herkkiä uhkamallille, ja lähes vakiomäärää koskeva havainto tarkoittaa, ettei mittakaava itses-sään suojaa [24]. Realistinen lähtö-kohta on **murtautumisoletus** (assu-me-breach): yhdistä ennaltaehkäisy, havainnointi ja reagointi sen sijaan, että luottaisit yhteen puolustuslin-jaan. ”Laboratorio”-onnistumisas-teet ali- tai yliarvioivat todellisen altistumisen [30, 31], ja mukautuvat hyökkääjät peittävät huomiosignaa-leja [35, 36] – kyse on kilpavaruste-lusta, ei ratkaistusta ongelmasta.

Heinä-lokakuun 2026 tulokset tuovat kaksi lisäopetusta. Yksinään harmittomat mutta yhdessä haital-liset myrkytykset kukistavat doku-menttikohtaisen tarkastuksen, joten hallintakeinojen on arvioitava haet-tua joukkoa kokonaisuutena [39, 40]. Lisäksi avointa verkkoa selaavat tai pit-käkestoista muistia ylläpitävät agentit perivät jokaisen käsittelemänsä sivun ja keskustelun eheyden, mikä laajentaa murtautumisoletuksen tietopohjasta agentin koko tietoravintoon [46–49].

Akateemiselle maailmalle tämä luo todellisen jännitteen avoimen tie-teen ja FAIR-periaatteiden kanssa: sama avoimuus, joka tekee datasta arvokasta, tekee siitä myrkytettä-vää. Parhaiten skaalautuvat lieven-nyskeinot ovat niitä, jotka säilyttävät avoimuuden – allekirjoitetut ja ver-sioidut aineistot, läpinäkyvä alkuperätieto, toistettavuus (joka toimii samalla havainnointina) sekä sel-keät kuratointi- ja arviointivastuut – datan sulkemisen sijaan.

LÄHTEET

[1] Biggio, B., Nelson, B., & Laskov, P. (2012). Poisoning Attacks against Support Vector Machines. ICML.

[2] Alber, D. A., et al. (2025). Medical large language models are vulnerable to data-poisoning attacks. Nature Medicine, 31(2), 618–626. doi:10.1038/s41591-024-03445-1.

[3] Gu, T., Dolan-Gavitt, B., & Garg, S. (2017). BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain. arXiv:1708.06733.

[4] Tran, B., Li, J., & Madry, A. (2018). Spectral Signatures in Backdoor Attacks. NeurIPS.

[5] Chen, B., et al. (2018). Detecting Backdoor Attacks on Deep Neural Networks by Activation Clustering. arXiv:1811.03728.

[6] Wang, B., et al. (2019). Neural Cleanse: Identifying and Mitigating Backdoor Attacks in Neural Networks. IEEE S&P.

[7] Gao, Y., et al. (2019). STRIP: A Defence Against Trojan Attacks on Deep Neural Networks. ACSAC.

[8] Liu, K., Dolan-Gavitt, B., & Garg, S. (2018). Fine-Pruning: Defending Against Backdooring Attacks on Deep Neural Networks. RAID.

[9] Koh, P. W., & Liang, P. (2017). Understanding Black-box Predictions via Influence Functions. ICML.

[10] Blanchard, P., et al. (2017). Machine Learning with Adversaries: Byzantine-Tolerant Gradient Descent (Krum). NeurIPS.

[11] Yin, D., et al. (2018). Byzantine-Robust Distributed Learning: Towards Optimal Statistical Rates (trimmed mean / median). ICML.

[12] Baracaldo, N., et al. (2017). Mitigating Poisoning Attacks on ML Models: A Data Provenance Based Approach. AISec.

[13] Zou, W., Geng, R., Wang, B., & Jia, J. (2025). PoisonedRAG: Knowledge Corruption Attacks to Retrieval-Augmented Generation of LLMs. USENIX Security 2025; arXiv:2402.07867.

[14] Zhong, Z., Huang, Z., Wettig, A., & Chen, D. (2023). Poisoning Retrieval Corpora by Injecting Adversarial Passages. EMNLP; arXiv:2310.19156.

[15] Xue, J., Zheng, M., Hu, Y., Liu, F., Chen, X., & Lou, Q. (2024). BadRAG: Identifying Vulnerabilities in Retrieval Augmented Generation of LLMs. arXiv:2406.00083.

[16] Chen, Z., Xiang, Z., Xiao, C., Song, D., & Li, B. (2024). AgentPoison: Red-teaming LLM Agents via Poisoning Memory or Knowledge Bases. NeurIPS; arXiv:2407.12784.

[17] Zhang, Y., et al. (2024). HijackRAG: Hijacking Attacks against Retrieval-Augmented LLMs. arXiv preprint.

[18] Liu, Y., et al. (2025). Poisoned-MRAG: Knowledge Poisoning Attacks to Multimodal Retrieval-Augmented Generation. arXiv:2503.06254.

[19] POISONCRAFT: Practical Poisoning of Retrieval-Augmented Generation for LLMs (2025). arXiv:2505.06579.

[20] Xiang, C., Wu, T., Zhong, Z., Wagner, D., Chen, D., & Mittal, P. (2024). Certifiably Robust RAG against Retrieval Corruption (RobustRAG). arXiv:2405.15556.

[21] Vassilev, A., Oprea, A., Fordyce, A., Anderson, H., Davies, X., & Hamin, M. (2025). Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. NIST AI 100-2e2025. doi:10.6028/NIST.AI.100-2e2025.

[22] OWASP (2025). Top 10 for Large Language Model Applications — LLM04:2025 Data and Model Poisoning.

[23] European Union (2024). Regulation (EU) 2024/1689 (Artificial Intelligence Act), Articles 10 and 15.

[24] Anthropic, UK AI Security Institute & The Alan Turing Institute (2025). Poisoning Attacks on LLMs Require a Near-constant Number of Poison Samples. arXiv:2510.07192.

[25] Edemacu, K., Shashidhar, V. M., Tuape, M., Abudu, D., Jang, B., & Kim, J. W. (2025). Defending Against Knowledge Poisoning Attacks During RAG (FilterRAG / ML-FilterRAG). arXiv:2508.02835.

[26] Cheng, Z., Sun, J., Gao, A., Quan, Y., Liu, Z., Hu, X., & Fang, M. (2025). Secure Retrieval-Augmented Generation against Poisoning Attacks. arXiv:2510.25025.

[27] Dekel, S., Tennenholtz, M., & Kurland, O. (2026). Addressing Corpus Knowledge Poisoning Attacks on RAG using Sparse Document Attention (SDAG). arXiv:2602.04711.

[28] Securing Retrieval-Augmented Generation: A Taxonomy of Attacks, Defenses, and Future Directions (2026). arXiv:2604.08304.

[29] MIRAGE: Misleading Retrieval-Augmented Generation via Black-box and Query-agnostic Poisoning Attacks (2025). arXiv:2512.08289.

[30] Hu, H., Jiang, Z., Lyu, Y., Zhang, J., Liu, Y., & Chow, K. (2026). Confundo: Learning to Generate Robust Poison for Practical RAG Systems. arXiv:2602.06616.

[31] Zhang, B., et al. (2025). Practical Poisoning Attacks against Retrieval-Augmented Generation (CorruptRAG). arXiv:2504.03957.

[32] Zhao, T., Chen, J., Ru, Y., Zhu, H., Hu, N., Liu, J., & Lin, Q. (2026). RAG Safety: Exploring Knowledge Poisoning Attacks to Retrieval-Augmented Generation (KG-RAG). Information Fusion, 127, 103900; arXiv:2507.08862.

[33] KEPo: Knowledge Evolution Poison on Graph-based Retrieval-Augmented Generation (2026). Proc. ACM Web Conference (WWW '26); arXiv:2603.11501.

[34] LogicPoison: Logical Attacks on Graph Retrieval-Augmented Generation (2026). arXiv:2604.02954.

[35] Dai, Y., Ji, Z., Li, Z., Li, K., & Wang, S. (2025). Disabling Self-Correction in Retrieval-Augmented Generation via Stealthy Retriever Poisoning (DisarmRAG). arXiv:2508.20083.

[36] Choudhary, S., Palumbo, N., Hooda, A., Dvijotham, K. D., & Jha, S. (2026). Through the Stealth Lens: Attention-Aware Defenses Against Poisoning in RAG (AV Filter / NPAS). OpenReview.

- [37] Cordon-MAS: Defending RAG against Knowledge Poisoning via Information-Flow Control (2026). arXiv:2605.26754.
- [38] Signed Memory with Smoothed Retrieval (SMSR): Certified Defence against Runtime Memory Poisoning in Persistent LLM Agent Systems (2026). arXiv:2606.12703.
- [39] Zhang, J., Chen, M., Ren, X., Zhang, Z., Shu, Y., Gao, Y., & Zhang, Z. (2026). InceptionRAG: Stealthy Poisoning Attack Against Retrieval-Augmented Generation. arXiv:2609.16818.
- [40] Pereira, P., Maia, E., & Praça, I. (2026). Micro-Collaborative Poisoning: A Distributed Attack on RAG Systems. arXiv:2609.21573.
- [41] Lu, H., Li, J., Zhu, X., & Li, X. (2026). ToxicRAG: Compromising Retrieval-Augmented Generation Systems via Single-Shot Knowledge Poisoning Attacks. arXiv:2609.11082.
- [42] Wang, Z., Zhu, Y., Dong, M., Lou, Y., Li, Y., Zhang, Z., Tong, W., Zhang, Y., Hua, J., & Zhong, S. (2026). PURPOSE: Poisoning Conflict Resolution in RAG via Proxy-Fact-Grounded Updates. arXiv:2608.04756.
- [43] Zhurekbay, A., Liu, T., & Li, F. (2026). DenialRAG: Single-Document RAG Poisoning via Embedded Parametric Denial. arXiv:2608.02678.
- [44] Kafi, A., & Khalil, A. A. (2026). RAG-NAROK: Retrieval-Aware Knowledge Corpus Poisoning in RAG with Source-specific Refutation. arXiv:2609.25469.
- [45] Gadey, V., Marey, Z., & Dmitrienko, A. (2026). CodePoisonRAG: Knowledge Poisoning Attacks on Retrieval-Augmented Code Generation. arXiv:2609.02774.
- [46] Zhang, T., Triedman, H., & Shmatikov, V. (2026). Deep-Research Agents Can Be Poisoned via User-Generated Content. arXiv:2605.24245.
- [47] Bi, Z., Wang, Q., Jiang, J., et al. (2026). Evaluating Deep-Search Agents under Hierarchical Web Evidence Poisoning (HAE-GEO). arXiv:2609.06027.
- [48] Torres, G., Shrestha, S., & Misra, S. (2026). When Agents Remember Too Much: Memory Poisoning Attacks on Large Language Model Agents (GhostWriter / AM-Sentry). arXiv:2607.06595.
- [49] Chen, X., Xie, X., Fu, W., Zhou, J., Yu, S., & Xuan, Q. (2026). MemSecBench: Tracking Agent Memory Poisoning from Persistence to Consequence and Repair. arXiv:2607.27080.
- [50] Muhamed, A., Diab, M. T., Smith, V., Ilyas, A., & Jagielski, M. (2026). Pick Your Poison: Learning to Select Poison Sets for Stronger LLM Backdoor Attacks (SAILS). arXiv:2609.15029.
- [51] Draganov, A., Dur, T. H., Bhongade, A., & Phuong, M. (2026). Phantom Transfer: Data Poisoning can Survive Data-Level Defences. arXiv:2602.04899.
- [52] Ren, Y., Zhao, Z., Fu, Y., Luo, X., Chang, Y.-C., & Lin, C.-T. (2026). When Context Bites: Detecting RAG Poisoning via Document-Level Attention Collapse (D-SCAN). arXiv:2608.06947.
- [53] Tan, X., Zheng, Y., Huo, C., Zhang, Y., Liu, Y., Luan, H., Yu, Z., Sun, X., Chen, P., & Dai, J. (2026). PRA-RAG: Provably Robust Aggregation in Retrieval-Augmented Generation against Retrieval Corruption. Findings of ACL 2026, pp. 36002–36017.
- [54] Apurba, K. A., Hasan, M. H., Moon, M. Z., Rahman, S. M. M., & Inomata, A. (2026). Defending Retrieval-Augmented Intrusion Detection Against Knowledge Poisoning and Prompt Injection. arXiv:2608.08100.
- [55] Biswas, S., Garcia Bourrée, J., Guerraoui, R., Jacovella, M., Kermarrec, A.-M., Peechara, S., de Vos, M., & Vujasinovic, M. (2026). Backdoor Mitigation in Decentralized LLM Fine-Tuning (Chorus). arXiv:2609.37367.
- [56] Huang, G., Puri, A., Boisvert, L., Drouin, A., Taslakian, P., Gella, S., & Pal, C. (2026). Backdoor Decontamination Dynamics in LLM Agents. arXiv:2608.11295.
- [57] Lin, T., Jin, G., Liu, Z., Wu, P., & Yu, L. (2026). Once Poisoned, Arbitrarily Controlled: A Programmable Backdoor in VLMs. arXiv:2608.10959.
- [58] OWASP GenAI Security Project (2025). OWASP Top 10 for Agentic Applications 2026 — ASI06: Memory & Context Poisoning.
- [59] European Union (2026). Regulation (EU) 2026/1744 (Digital Omnibus on AI) amending Regulation (EU) 2024/1689. OJ L, 24 July 2026.

KIRJOITTAJA:



KIMMO K. KASKI

Kimmo Kaski toimii emeritusprofessorina Aalto-yliopiston Perustieteiden korkeakoulussa, ja hänet tunnetaan kansainvälisesti tunnustettuna Laskennallisen Tieteen tutkijana. Hän on erikoistunut monimutkaisten järjestelmien tutkimukseen, käsittäen muun muassa sosiaaliset ja informaatioverkostot, ja hyödyntää työssään sekä suurten tietoaaineistojen data-analytiikkaa että laskennallisia mallinnusmenetelmiä.

Vaatimustenmukaisuus energijärjestelmän reunalla

KYBERTURVALLISUUDEN HALLINTO HAJAUTETUISSA ENERGIARESURSSSEISSA

Tiivistelmä Cyberwatch
Finlandin julkaisemasta
White paper raportista
Lokakuu 2026

1. Hallinto kysymyksenä

Energiantuotannon vähähiilistäminen ja monipuolistuminen haastavat kyberturvallisuuden hallintomallit, jotka on alun perin rakennettu keskitettyä sähköverkkoa varten. Kun energijärjestelmät hajautuvat, nojaavat yhä enemmän ohjelmistoihin ja ovat yhä vähemmän keskitetysti ohjattuja, järjestelmän toimintavarmuus ja sen digitaalisen kerroksen turvallisuus kytkeytyvät perustavanlaatuisesti toisiinsa. Kyberhyökkäykset ovat tahallisia ja

vaikutuksiin tähtääviä tekoja, joilla tavoitellaan operatiivisia, taloudellisia ja viime kädessä poliittisia päämääriä. Siksi hallinto on välttämätön täydennys tekniikkapainotteiselle johtamiselle. Raportissa kysytään, miten kyberturvallisuusvelvoitteiden noudattamisen vastuu voidaan kohdentaa, miten noudattaminen voidaan todentaa ja miten se voidaan panna täytäntöön hajautetun energijärjestelmän toimijakentässä, joka on huomattavasti monimuotoisempi kuin se, jota varten nykyiset sääntelyjärjestelmät on luotu. Raportti on

tarkoitettu ajatusten herättäjäksi julkisen politiikan suunnittelijoille ja energia-alan hallinnolle, ei velvoittavaksi toimintamalliksi.

Tarkastelemme energia-alan ja hajautettujen energiaressurssien (distributed energy resources, DER) kyberturvallisuutta hallinnon eikä tekniikan kysymyksenä: kuka asettaa vaatimukset, kuka valvoo niiden noudattamista ja miten toimivalta ja voimavarat jakautuvat instituutioiden ja alueiden kesken. Standardeissa on jo määritelty, millainen on sisäänrakennetusti turvallinen, nollaluottamukseen perustuva ja toimitusketjultaan todennettu infrastruktuuri. Ne eivät kuitenkaan ratkaise, kenen vastuulla on edellyttää, rahoittaa ja valvoa näitä ratkaisuja, eivätkä sitä, miten vastuun pitäisi erota kypsien ja kehittyvien sääntelijöiden ja toimialojen välillä.

Hallinto koskee järjestyksen sääntöjä ja periaatteita sekä sitä, miten valta järjestelmässä organisoidaan. Se suuntaa yksittäisiä, sinänsä oikeutettuja vaatimuksia kohti yhteistä arvoa. Hallinto on aatteellista, johtaminen järjestelmällistä ja organisatorista; ne ovat toisistaan erillisiä mutta erottamattomia. Kantia mukaillen johtamisjärjestelmä ilman hallinnon ihanteita on sokea, ja hallinto ilman järjestelmällistä ja organisatorista ilmentymää jää tyhjäksi. Raportti noudattaa riskiperusteisen lähestymistavan sijaan varovaisuusperiaatetta ja sitoo vastuun toimijan asemaan järjestel-

mässä: on tärkeämpää tietää, mitä on suojattava, kuin keneltä.

Pitäisikö hallintoa koskevat suositukset siis sovittaa alueellisesti, vai ovatko perusasiat alueesta riippumattomia? Vastauksemme on: molempia, mutta eri tasoilla. Nollaluottamusarkkitehtuuri, hankinnat, jotka edellyttävät sisäänrakennettua tietoturvaa, komponenttiluettelot ja määräaikaikoihin sidottu häiriöilmoittaminen toimivat kaikkialla samalla tavalla, koska ne vastaavat teknologian ominaisuuksiin. Myös YK:n hallitusten asiantuntijaryhmän (UN GGE) vuoden 2015 normit kriittisen infrastruktuurin suojaamisesta, toimitusketjujen eheydestä ja CERT-ryhmien toiminnan koskemattomuudesta ovat vakiintuneita odotuksia, ja YK:n avoin työryhmä (Open-Ended Working Group) vahvisti ne uudelleen heinäkuussa 2025.

Yleispätevä ei kuitenkaan tarkoita itsestään toteutuvaa. Alueiden välillä eroaa hallinnon arkkitehtuuri: täytäntöönpanokyky, institutionaalinen luottamus, jakeluverkko- ja DER-tason valvonnan kypsyys sekä rahoituksen ja erikoistuneen työvoiman saatavuus. Analyysi jäsentyy kuuden hallintoperiaatteen varaan, jotka pohjautuvat CISA:n Performance Goals 2.0 -tavoitteisiin ja DCAF:n julkaisuun Guide to Good Governance in Cybersecurity. Periaatteet ovat oikeudellinen ja poliittinen kehys; institutionaalinen toimivalta ja vastuuvollisuus; riskien hallinta; operatiivinen suorituskyky;

toimitusketjun ja teknologian turvallisuus; sekä yhteistyö ja valvonta.

2. Energiajärjestelmän hajautettu reuna

Sähköjärjestelmän ohjaus on siirtynyt muutamista suurista, fyysisesti suojatuista laitoksista lukuisiin pienempiin, ohjelmisto-ohjattuihin ja etähallittuihin kohteisiin. Kansainvälinen energiajärjestö IEA määrittelee hajautetut energiaressurit pienimuotoisiksi energiaressusseiksi, jotka sijaitsevat yleensä lähellä sähkön käyttöpaikkaa. Niitä ovat katto-aurinkovoimalat, mittarin takana olevat akut, sähköautot ja niiden latauslaitteet, kysyntäjoustolaitteet sekä niitä ohjaavat mittarit ja ohjaimet. Resursseja yhdistää sijainti: ne ovat asiakkaan mittarilla tai sen takana eli sen alueen ulkopuolella, jota verkko-yhtiöt ovat perinteisesti hallinneet. Samalla ne ovat siirtyneet marginaalista järjestelmän rakenteelliseksi osaksi. Vuosittain käyttöön otetun aurinkosähkökapasiteetin arvioidaan maailmanlaajuisesti kasvaneen 145 gigawatista vuonna 2020 ennätykselliseen 602 gigawattiin vuonna 2024, ja kumulatiivinen kapasiteetti nousi vuonna 2025 noin 2 380 gigawattiin.

Hallinnon ongelma on omistajuus eikä teknologia. Suuret tuotanto- ja siirtokohteet kuuluvat säännellyille verkkoyhtiöille ja luvanvaraisille tuottajille, joihin perinteiset ohjauskeinot ulottuvat. Hajautetut resurssit

taas kuuluvat kotitalouksille, kiinteistöjen ylläpitäjille, ajoneuvokantojen hallinnoijille ja aggregaattoreille, jotka tarjoavat yhdistettyä kapasiteettia markkinoille virtuaalivoimailaitoksina. Aggregaattori voi ohjata laitekantaansa ilman minkäänlaista sääntelysuhdetta siihen verkonhaltijaan, jonka verkon vakaus siitä riippuu, ja vastuu DER-kerroksesta on usein ratkaisematta. IEA tunnistaa näkyvyyssaukon sekä rakenteellisen ristiriidan laitteitaan itse käyttävän kansalaisen etujen ja järjestelmän tarpeiden välillä. Sääntelijöillä ja järjestelmävastaavilla ei ole tietoa mittarin takana olevista resursseista eikä pienjänniteverkkojen seurantaa. Ellei hallinto rankaise tai palkitse toimijoita heidän käyttäytymisensä perusteella, monet laitteet jäävät päivittämättä.

Kun verkkosäännöt edellyttävät IEA:n suosituksen mukaisesti kehittyneitä vaihtosuuntaajatoimintoja liittymisen ehtona, liittämisvaiheeseen syntyy portti, joka on luonteva väylä todennetulle laitetunnisteelle. Jos aggregaattoreiden markkinaroolit virallistetaan määrittelemättä niiden turvallisuusvelvoitteita, laitteiden kohdalla jo tehty virhe toistuu yhtä kerrosta ylempänä. DER-kasvun suunta on maailmanlaajuinen, mutta sen tahti ja instituutioiden valmius hallita sitä vaihtelevat alueittain.

3. Kyberfyysinen uhkaympäristö

Operatiivista teknologiaa (OT) aiemmin suojannut fyysinen eristys on katoamassa, kun etävalvonta, pilvipohjainen laitekannan hallinta ja kolmansien osapuolten huolto moninkertaistavat yhteydet yritysten tietojärjestelmiin ja ulkoisiin verkoihin. Keskitetyt osa-alueet, kuten ydinvoima ja kantaverkon siirto, toimivat tiukkojen valvontajärjestelmien alaisina, mutta jakeluinfrastruktuuri, kuluttajalaitteet ja keskitetysti hallitut uusiutuvan energian laitekannat eivät. Hyökkäyspinnan määrittää siksi vähemmän laitteiden

määrä kuin ne ohjaussuhteet, joihin operaattorit, laitetoimittajat, aggregaattorit ja asiakkaat luottavat niitä kyseenalaistamatta. Vuosina 2010–2024 energia-ala oli televiestinnän jälkeen toiseksi yleisin hyökkäysten kohde, ja noin kaksi kolmasosaa tekijään yhdistetyistä operaatioista jäljitettiin Kiinaan, Venäjälle ja Iraniin. Altistuminen keskittyy sinne, missä geopolittiset konfliktit ja heikosti suojattu digitaalinen riippuvuus kohtaavat.

Perusmenetelmiin kuuluvat tunnistetietojen varastaminen, etäyhteyksien hyväksikäyttö, kiristyshaittaohjelmat, palvelunesto, hyökkäykset sekä järjestelmän omia työkaluja hyödyntävä (living-off-the-land) pysyvä läsnäolo. Vakavia vahinkoja voi seurata jo pelkän toimistoverkon vaarantumisesta. Huhtikuussa 2025 Venäjä-mielisiin ryhmiin kytkeytyneet toimijat kaappasivat Norjassa sijaitsevan Risevatenin vesivoimapadon ohjauksen ja pitivät sen venttiiliä täysin auki tuntikausia ennen kuin tunkeutuminen havaittiin. Joulukuussa 2025 torjuttiin koordinoitu operaatio, joka kohdistui hajautettuun tuotantoon yli kolmessakymmenessä kohteessa Puolassa. Se oli European Repository of Cyber Incidents -tietokannan mukaan laatuaan ensimmäinen, ja se vahvisti, että kyvykkäät hyökkääjät pitävät DER-kerrosta yhtenäisenä kohteena.

Valtiollisten ja ei-valtiollisten toimijoiden välinen raja hämärretään tarkoituksella. Joulukuussa 2025 julkaistussa yhteisessä tiedotteessa itseään hakkeriaktivisteiksi kutsuva CARR-ryhmä, jonka jäsenet perustivat Norjan tunkeutumisen taustalla olleen ryhmän, yhdistettiin Venäjän sotilastiedustelun yksikköön 74455. Puolustuksen perustason on siksi oltava riippumaton siitä, millä nimellä tai minkä lipun alla hyökkääjä esiintyy. Tekoäly lisää hyökkääjien tuottavuutta, vaikka näyttö autonomisista, sähköverkkoa häiritsevistä tekoälyhaittaohjelmista on yhä heikkoa ja kampanjoiden kiihtyvä tahti on jo sinänsä riittävä

syy toimia nopeammin kuin vaatimustenmukaisuuden syklit sallivat. NIS2-direktiivin laajamittaisuuden kynnyksen alle jäävät häiriöt kuormittavat yhteenlaskettuina reagointikykyä, ja yksittäisiin vakaviin tapahtumiin mitoitettut ilmoitusjärjestelmät aliarvioivat uhan, jonka merkittävyys on yksittäisten vakavien tapahtumien kasautumisessa.

Onnistuneiden kyberoperaatioiden taustalla toistuu kolme mahdollistavien olosuhteiden luokkaa, joista vain yksi on tekninen. Infrastruktuuri, teknologia ja organisaatio kattaa eriyttämättömät turvallisuustasot, vanhentuneet laitteet ja leväperäisen päivityskäytännön. Valtionhallinto, politiikka ja lainsäädäntö kattaa jälkeen jääneet säädösheykset ja ratkaisemattoman vastuunjaon, mikä näkyy DER-aggregoinnin ja täytäntöönpanokyvyn aukkoina. Sosiokulttuuriset ja inhimilliset tekijät kattavat hajautuneeseen omistajuuteen liittyvän vähäisen tietoisuuden ja häiriöiden sietämisen. Hallintostrategia, joka on laadittu vastaamaan vain yhteen luokkaan, jättää muut avoimiksi.

4. Reunan vaatimustenmukaisuuskehys

Reunan ja ytimen käsitteet kuvaavat rakenteellista suhdetta. Ydin muodostuu järjestelmistä, jotka jo kuuluvat vaatimustenmukaisuutta koskevan sääntelyn piiriin, kuten NERC CIP -vaatimusten alaisista suurista sähköjärjestelmän kohteista, NIS2-direktiivin mukaisista keskeisistä toimijoista ja Kiinan kyberturvallisuuslain tarkoittamasta kriittisestä tietoinfrastruktuurista. Reuna jää näiden rajojen ulkopuolelle. Raja siirtyy ulospäin DER-resurssien yleistessä, mutta epäsymmetria säännellyn ytimen ja sääntelemättömän reunan välillä säilyy edelleen. Ytimessä vaatimustenmukaisuus on hallittavissa, koska pienellä joukolla luvanvaraisia toimijoita on kohteita, jotka sääntelijät voivat tunnistaa ja tarkastaa ja joihin ne voivat kohdis-



taa seuraamuksia. DER-kerroksessa jokainen näistä edellytyksistä kääntyy päinvastaiseksi. Säätely, joka kohtelee reunaa ytimen pienoisversiona, epäonnistuu, koska kyse on laadullisesta eikä mittakaavaan liittyvästä ongelmasta. Ytimeen voidaan myös hyökätä reunan kautta: vaarantunut aggregaattori voi ohjata kymmeniä tuhansia laitteita yhtä aikaa ja aiheuttaa kuormitustapahtuman, jonka verkonhaltija näkee fyysisenä häiriönä ilman näkyvää kybersyytä.

Kansainväliset standardit tarjoavat teknisen perustan. IEC 62443 -standardisarja vastaa hyvin DER-toimijoiden kenttää: siinä asetetaan velvoitteita järjestelmien omistajille, järjestelmäintegraattoreille – aggregaattorit ja asentajat mukaan lukien – sekä komponenttivalmistajille, ja sen turvatorakenne mahdollistaa velvoitteiden porrastamisen kriittisyyden mukaan. NIST CSF 2.0 tuo mukaan hallintoa koskevan Govern-toiminnon, ja ISO/IEC 27001 tarjoaa aggregaattoreille auditoitavan polun. Mikään niistä ei kuitenkaan ratkaise kysymystä säätelyvallasta, eikä mitään niistä ole suunniteltu yksittäiselle laitteen omistajalle. Ratkaisu on siirtää velvoitteet ylemmälle tasolle, eli valmistajalle tuotelainsäädännön kautta, asentajalle verkkoon liittämissä vaatimusten kautta ja aggregaattorille markkina- ja lupaehtojen kautta. Näin laitteet täyttävät vaatimukset jo verkkoon liitettäessä, ilman vaatimusta laitteenomistajan olla se pätevä kyberturvallisuustoimija.

Ehdotamme neljään pilariin perustuvaa vaatimustenmukaisuuden vähimmäisarkkitehtuuria.

Soveltamisala kohdentaa velvoitteet toimijan roolin ja kyvykkyyden eikä omaisuuden omistajuuden perusteella. Toimijoita ovat valmistaja, asentaja, aggregaattori, jakeluverkonhaltija ja yksittäinen omistaja. Aggregaattori on vaatimustenmukaisuuden keskeinen solmukohta, ja jakeluverkonhaltijan velvoite koskee näkyvyyttä eli todennet-

tua luetteloa verkkoon liitetyistä kohteista.

Perusvelvoitteet määritellään tavoiteltavina lopputuloksina, ja verkkoon liitettyjen DER-resurssien vähimmäistaso on IEC 62443 -standardin turvataso 2 (Security Level 2). Velvoitteisiin kuuluvat oletusarvoisesti turvaliset laitteet, joilla on päivitystuki ja ohjelmistojen materiaaliluettelot (SBOM); liittämisvaiheen käyttöönottotarkastus, joka on tehokkain mutta vähiten hyödynnetty käytettävissä oleva keino, sillä se ei edellytä uutta toimivaltaa vaan ainoastaan päivitetyn verkkosäännön; sekä aggregaattoreiden lupaehtona tietoturvalisuuden hallintajärjestelmä ja häiriöilmoitusvelvollisuus.

Todentaminen vastaa toimijoiden moninaisuuteen esimerkiksi tuotesertifiointilla, käyttöönotto-tarkastuksilla, aggregaattoreiden kolmannen osapuolen auditoinnilla sekä safe harbour -suojalla turvatulla häiriöilmoittamisella. Tässä tarkoitetaan ilmoittajan vastuuvapausuojaa, jossa toimija, joka ilmoittaa kyberhäiriöstä tai haavoittuvuudesta vilpittömästi, ei joutuisi ilmoituksen vuoksi sakkojen, sanktioiden tai muun vastuun kohteeksi.

Vastuuvellisuus kohdistuu toimijaan, jolla on parhaat edellytykset toimia, ja asettaa vaatimusten noudattamisen markkinoille pääsyn ehdoksi sen sijaan, että nojattaisiin jälkikäteisiin seuraamuksiin.

Vaatimustenmukaisuuteen perustuvilla strategioilla on taipumus tuottaa sitä, mitä Power (2007) kutsuu organisoiduksi tekopyhyydeksi, eli missä on muodollisia rakenteita, jotka tyydyttävät auditoijia, mutta jättävät operatiivisen altistumisen ennalleen. Ensimmäinen edellytys on DER-kerrokselle nimetty vastuuviranomainen. Sitä ei synny energiasääntelijöiden, kyberturvallisuusviranomaisten, tuoteturvallisuusviranomaisten ja markkinasääntelijöiden nykyi-

sen pirstaleisen työnjaon pohjalta. Kansallinen kyberturvallisuus- tai energiaturvallisuusstrategia on väline, jolla tämä kirjataan poliittisella tasolla. Se on tasapainoinen punninta, joka valitsee vaihtoehtojen välillä, priorisoi tavoitteita, kohdentaa resursseja ja vastuita sekä legitimoit valitun suunnan. Oikeudenkäyttöalue, jolta tällainen strategia puuttuu, ilmentää oikeudellispoliittista mahdollistavaa edellytystä puhtaimmillaan. Strategia on räätälöitävä eikä tuotava muualta, ja sen hallinta perustuu optimaaliseen kohdentamiseen eikä maksimaaliseen tavoitteluun. Keskusviranomaisen ohjaa ja valvoo, kun taas toimeenpano säilyy asiantuntijoilla, jotka ovat lähimpänä suojattavia kohteita. Keskittämisen ja hajauttamisen välinen tasapaino sovitetaan harkiten, ja suhtaudumme epäillen siihen, että mikään yksittäinen virasto pystyisi hallitsemaan kyberturvallisuuden ja hajautetun energian yhteenlaskettua moninaisuutta. Arvioinnin on mitattava vaikuttavuutta eikä panoksia ja tuotoksia.

Toimeenpano edellyttää lisäksi harkittua yhdistelmää velvoitteita, kannustimia ja tiedottamista; valmiuksien kehittämistä, sillä maailmanlaajuisesti alalta puuttuu noin 3,4 miljoonaa ammattilaista; sekä elinkaarivelvoitteita, koska vaatimustenmukaisuus on prosessi eikä tila. Vuoden 2024 perustason mukaisesti asennetuissa laitteissa on vuoteen 2028 mennessä laiteohjelmistoja, joissa on tunnettuja haavoittuvuuksia, elleivät päivitysaikataulut ja uudelleenvarmennukset pidä velvoitteita ajan tasalla.

5. Alueelliset havainnot

Poliittiset kulttuurit, resurssit ja geopolitiikka vaikuttavat siihen, miten sitovat ja vapaaehtoiset ohjauskeinot painottuvat ja millaiset roolit valtiolla, yksilöllä ja yksityisellä sektorilla on. Neljän pilarin valossa alueista piirtyy seuraava kuva.

ALUE	PISIMMÄLLE EDENNYT	DER-KERROKSEN KESKEISIN PUUTE
Euroopan unioni	Horizontaalinen NIS2-direktiivi ja alakohtainen kyberturvallisuutta koskeva verkkosäätö (Network Code on Cybersecurity); kyberresilienssisäädös ulottuu valmistajiin; valvontaviranomaisten sakot ja CE-merkinnän peruuttaminen.	Toimijakohtaiset kynnysarvot alittavat aggregaattorit sekä asentajat ovat pääosin soveltamisalan ulkopuolella; täytäntöönpanon laatu riippuu jäsenvaltioiden epätasaisista valmiuksista.
Yhdistynyt kuningaskunta	Energia-alan kyberturvallisuusstrategia 2026 (Energy Sector Cyber Security Strategy 2026) laajentaa soveltamisalan kaikkiin Ofgemin luvanhaltijoihin; perustasona Cyber Essentials, ja kriittiset toimittajat nimetään vuoteen 2030 mennessä.	Soveltamisala rajoittuu toistaiseksi NIS-toimijoihin; kattavammat täytäntöönpanokeinot riippuvat Cyber Security and Resilience Bill -lakiesityksestä.
Yhdysvallat	Yksityiskohtaiset ja täytäntöönpanokelpoiset NERC CIP -velvoitteet Bulk Electric System -järjestelmälle, joka kattaa noin 10–20 % fyysisestä laitekannasta.	Liittovaltiotason soveltamisala ei kata järjestelmällisesti siirtoverkon kynnyn alittavia kohteita; jakeluverkkojen perustasot ovat vapaaehtoisia; liittovaltio linjaa säätelyn purkua; CIRCIA-säännös on viivästynyt; CISA:n resursseja on supistettu.
Aasian ja Tyynenmeren alue	Kiinan kriittistä tietoinfrastruktuuria (CII) koskeva säätely, jossa vuodesta 2026 alkaen kymmenkertaiset seuraamukset ja henkilökohtainen vastuu; Intian vuoden 2025 CEA-asetusluonnos; Australian SOCI-laki ja yhtenäinen CISC-viranomainen.	Aggregaattorit ja asentajat jäävät SOCI- ja CII-säätelyn ulkopuolelle; Intian täytäntöönpanokyky on haasteellinen satojen verkkoyhtiöiden kentässä; ASEAN-maissa ei ole sitovaa kehystä.
Afrikka	Malabon yleissopimus voimassa vuodesta 2023; Nigerian CNII Order 2024 ja Kenian CII Regulations 2024 määrittelevät soveltamisalan.	Velvoitteet ovat periaatetasolla; DER-laitteistolle ei ole perustasoa; todentamiskyky puuttuu; kehityspankkien rahoitusehdot ovat tärkein vipu.
Latinalainen Amerikka ja Karibia	Chilen laki 21.663: 915 elintärkeää toimijaa (Operators of Vital Importance), joista 307 sähköalalla; sitova säätely ja ANCI:n sakotusvaltuudet.	Aggregaattorit ja asentajat eivät ole erillisiä toimijoita; Brasilian viranomainen on vielä perustamatta; muualla nojataan kehityspankkien vipuvaikutukseen, ja toimeenpantuja strategioita on vähän.

Taulukko 1. Koottu pääraportin luvusta 5 ja taulukosta 6, joissa lähteet on esitetty

Edistys keskittyy suurten toimijoiden soveltamisalan määrittelyyn; yksikään lainkäyttöalue ei ole toteuttanut kaikkia neljää pilaria DER-kerroksessa. Mikään lainkäyttöalue ei ole myöskään asettanut aggregaattoreiden ja virtuaalivoimalaitosten vaatimustenmukaisuutta markkinoille pääsyn ehdoksi, vaikka aggregaattori on vaatimustenmukaisuuden keskeinen solmukohta. DER-laitteiden tuotesertifiointi on käytössä vain EU:ssa, eikä sekään ulotu laitteisiin, jotka hankitaan EU:n markkinakanavien ulkopuolelta. Toimivilla vastuuvellisuusmekanismeilla, kuten Chilen sakotusvaltuuksilla, Australian lupahdoilla ja EU:n valvontaseuraamuksilla, on yhteinen rakenne: markkinoille pääsy edellyttää vaatimustenmukaisuutta ja nii-

den noudattamista sen sijaan, että rikkomuksista rangaistaisiin vain jälkikäteen. Puutteet johtuvat alueittain vaihtelevista olosuhteista, joita ovat täytäntöönpanokyky, institutionaalinen luottamus, DER-tason valvonnan kypsyys sekä rahoitus ja työvoima. Tekniset perustasot ovat yleispäteviä, mutta niiden täytäntöönpanoon tarvittava arkkitehtuuri riippuu alueesta. Pisimmälle edenneet lainkäyttöalueet ovat tehneet saman poliittisen valinnan, ja se on myös muiden tehtävissä.

6. Suositukset

Välineet DER-reunan hallintaan ovat olemassa, mutta useimmilla lainkäyttöalueilla ei ole tehty poliittisia

päätöksiä vaatimusten noudattamisen edellyttämisestä. Tunnistamme neljä strategista tehtävää vähimmäistason toimenpiteille. Kaikkialla sovellettavat toimintalinjat on merkitty tunnuksella **[Yleinen]** ja paikallisiin tavoitteisiin, valmiuksiin, luottamukseen tai resursseihin sovitettavat toimintalinjattunnuksella **[Alueellinen]**.

Tehtävä 1: Yhteisen teknisen vähimmäistason luominen (pilari 2; infrastruktuuriin liittyvä mahdollistava olosuhde). **[Yleinen]** Hankinnoissa olisi syytä edellyttää sisäänrakennettua tietoturvaa ja oletusarvoisesti todennettuja yhteyksiä, kriittisten komponenttien ohjelmisto- ja laitteistomateriaaliluetteloita sekä nollaluottamukseen

perustuvaa todennusta ja segmentointia kaikissa IT- ja OT-ympäristöjen rajapinnoissa. Sopimuksissa kannattaisi viitata suoraan standardeihin IEC 62443, ISO/IEC 27019 tai NIST SP 800-82 ja edellyttää alkuperän sekä päivitystuen aikataulun ilmoittamista. Vanhoille laitteille tulisi antaa resursoitu siirtymäaika rahoittamattoman veloitteen sijaan.

Tehtävä 2: Jakeluverkon ja DER-kerroksen aukon sulkeminen (pilarit 1 ja 3). [Yleinen] Aggregaattorit, sähköautojen latausoperaattorit ja älymittarialustat tulisi tuoda olemassa olevien kyberturvallisuusvelvoitteiden piiriin. [Alueellinen] Joillakin alueilla siirtoverkon valvonta on vahvaa mutta jakeluverkon säännöt heikkoja, kuten Pohjois-Amerikassa. Niillä olisi perusteltua ulottaa nykyistä valvontaa alemmas sen sijaan, että luotaisiin rinnakkainen ja heikompi järjestelmä. [Alueellinen] Siellä, missä DER-resurssien kasvu ohittaa valvontavalmiudet, olisi hyvä asettaa etusijalle todennettu laitetunnistus ja perustason päivitykset. Ne ovat tärkeämpiä kuin kattava kehys, jota ei pystytä panemaan täytäntöön. Kryptografinen laitetunniste kannattaisi tehdä liittämisen ehdoksi, ja laitteiden omistajille tulisi toimittaa vähimmäistason tietoturvatiedote.

Tehtävä 3: Toimitusketjujen auditointiviksi tekeminen (pilarit 3 ja 4). [Yleinen] Kriittisten laitteistojen ja laiteohjelmistojen osalta tulisi edellyttää komponenttitason alkuperätietojen ilmoittamista. [Alueellinen] Siellä, missä hankintojen vipuvaikutus on vähäinen, kysyntää voitaisiin koota yhteen alueellisten konsortioiden tai kehityspankkien rahoitusehtojen avulla. Siellä, missä vipuvaikutusta on, kuten EU:ssa ja Yhdysvalloissa, ilmoitusvelvollisuus olisi hyvä ulottaa jakeluverkon ja DER-resurssien laitteistoihin.

Tehtävä 4: Täytäntöönpano- ja ilmoituskyvyn vahvistaminen siellä missä se on heikointa (pilari 4;

oikeudellis-poliittinen mahdollistava olosuhde). [Alueellinen] EU:ssa olisi tarkoituksenmukaisempaa rahoittaa kansallisia valvontaviranomaisia kuin lisätä keskitettyjä sääntöjä. Yhdysvalloissa taas osavaltioiden sääntelyä voitaisiin yhdenmukaistaa esimerkiksi kannustimin. Afrikassa sekä osassa Aasian ja Tyynenmeren aluetta ja Latinalaista Amerikkaa kannattaisi hyödyntää avunantajien ja kehityspankkien rahoitusta sääntelyvalmiuksien rakentamisessa. [Yleinen] Rankaisevat ilmoitusjärjestelmät tulisi korvata hyvässä uskossa ilmoittavien safe harbour-suojalla. Parlamentaarista valvontaa olisi syytä vahvistaa, ja alan hallinto olisi hyvä kirjata kansalliseen kyberturvallisuus- tai energia-alan turvallisuusstrategiaan. Strategian tulisi kattaa nimenomaisesti DER-kerros, se tulisi räätälöidä kyseiselle lainkäyttöalueelle, ja sitä tulisi hallita koko sen elinkaaren ajan.

Toimeenpanoa tulee vaiheistaa. Ensimmäisen vuoden aikana olisi hyvä nimetä vastuuviranomainen, määritellä toimijaroolien luokittelu, päivittää verkkosäännöt käyttöönototarkastuksella ja julkaista turvatasoon 2 perustuva kansallinen perustaso. Toisen ja kolmannen vuoden aikana voitaisiin ottaa käyttöön tuotesertifiointi ja perustaa joustoresurssien rekisteri, joka toimisi samalla kohdeluettelona. Samassa vaiheessa voitaisiin aloittaa aggregaattoreiden auditoinnit. Kolmannen vuoden jälkeen olisi aika ottaa käyttöön markkinoille pääsyn ehdollisuus, päivitysaikataulut ja uudelleenvarmennus sekä ajoittaa ensimmäinen sääntelyn arviointi.

Edistystä olisi syytä mitata vaikutuksilla. Mittareita voisivat olla esimerkiksi se, kuinka suuri osa uusista DER-kohteista läpäisee käyttöönototarkastuksen ja kuinka suurella osalla aggregaattoreista on todennettu sertifiointi. Jos lainkäyttöalue ei pysty raportoimaan tällaisilla mittareilla, sen voidaan katsoa ottaneen kehityksen käyttöön vain paperilla. Yritysjohdon ja operaattoreiden kan-

nattaisi asettaa etusijalle tehtävät 1 ja 2, päätöksentekijöiden ja sääntelijöiden tehtävä 4 sekä sijoittajien ja rahoittajien tehtävä 3.

7. Johtopäätökset

Energiajärjestelmiin lisätään kohteita hajautetulle reunalle nopeammin kuin hallinto pystyy seuraamaan – ja kyberasioille tyypilliseen tapaan myös vastustajat ovat huomanneet tämän. Edellä esitetty neljän pilarin kehys ei tuo uutta standardia. Sen sijaan se kysyy ja vastaa, kenen on noudatettava vaatimuksia, mitä vaatimuksia, miten noudattamista arvioidaan ja mitä seuraa, jos niitä ei noudateta. Tavoitteet ovat jokaisella alueella toimeenpanoa edellä, ja aggregaattoreiden markkinoille pääsyn sitominen vaatimusten noudattamiseen on tehokain käytettävissä oleva toimenpide ilman uutta täytäntöönpanokoneistoa. Vaatimustenmukaisuus ei tuota turvallisuutta automaattisesti. Lääke organisoituun tekopyhyyteen ei olekaan lisätä vaatimuksia vaan tehdä parempaa toimeenpanon suunnittelua.

DER-resurssien vaatimustenmukaisuus on tunnustettava kansalliseksi kysymykseksi, sillä sääntelemättömät reunan kohteet altistavat valtion infrastruktuurin riskeille ylittämättä kansallisen turvallisuuden tai kriittisen infrastruktuurin kynnysarvoja. Energiajärjestelmän reuna toimii jo nyt operaatioalueena. Aggregaattoreiden vaatimustenmukaisuuden pitäisi olla markkinoille pääsyn edellytys jokaisella lainkäyttöalueella, joka on avannut markkinansa aggregoinnille, ja oikeudellinen toimivalta siihen on usein jo olemassa. Kehityspankkien energiainfrastruktuurille myöntämän rahoituksen vakioehtoihin pitäisi sisällyttää kyberturvallisuusvaatimusten noudattaminen. Lisääntyvä tai kypsempi hallinto kun ei automaattisesti tuota resilienssiä, mutta harkittu ja tarkoituksenmukainen hallinto tuottaa sitä.



Cyberwatch Finland

KUUKAUSIKATSAUS

LOKAKUU/2026



Cyberwatch Finland liittyi osaksi Netum Groupia 21.4.2026.



Tässä katsauksessa

Tässä kuukausikatsauksessa tarkastelemme edellisen kuukauden merkittävimpiä kybermaailman tapahtumia ja sidomme ne laajempiin kokonaisuuksiin. Katsaus jakautuu neljään tarkastelukulmaan: kuukauden merkittävimpiin kybermaailman tapahtumiin,

ilmiöihin, joita haluamme erityisesti korostaa, kokonaisuuksiin, joiden kehitystä kannattaa seurata sekä tuoreimpiin tietoihin tekoälyn vaikutuksesta kyberturvallisuuteen.



1 TAPAHTUMIA KYBERMAISEMASSA

Kansainvälinen politiikka ja valtioiden väliset suhteet heijastuivat jälleen syyskuussa kybermaailmaan. Euroopassa kyberulottuvuus näkyi selkeimmin Saksan Saksi-Anhaltin osavaltiovaaleissa, joissa Venäjän sotilastiedustelu GRU:hun liittyvän Storm-1516-ryhmän epäiltiin pyrkineen vaikuttamaan vaalien lopputulokseen informaatiovaikuttamisen kautta. Myöskään Ruotsissa 13.9. pidetyt valtiopäivät eivät sujuneet häiriöttä. Niiden yhteydessä tunnistettiin yli 8500 epäilyttävää X-tiliä, minkä lisäksi perättömiä väitteitä vaalivilpistä levisi teknisen virheen jälkeen. Vaalihäirintää ei Ruotsin tapauksessa kuitenkaan yhdistetty Venäjään, ja maan viranomaiset arvioivat, etteivät vaalit olleet Venäjälle korkea prioriteetti. Norjassa maan suurkäräjät joutuivat Venäjä-mielisen Server Killers -haktivistiryhmän palvelunestohyökkäyksen kohteeksi 14.9., mikä oli jatkoa jo elokuun lopusta jatkuneelle hyökkäyskampanjalle. Viitteitä Venäjän hybridioperaatioiden kiihtymisestä on myös kyberulottuvuuden ulkopuolella.

Globaalisti Yhdysvaltain ja Kiinan välinen huipukokous 23.–26.9. ei tuottanut sitovia sopimuksia, mutta osapuolet sopivat uuden kanavan perustamisesta tekoälyn liittyvien häiriötilanteiden käsittelyyn sekä erillisen tekoälydialogin käynnistämisestä. Tämä osoittaa tekoälyn nousseen tärkeäksi turvallisuuskysymykseksi myös suurvaltojen välisissä suhteissa. Aasiassa Japani tunnisti ja onnistuneesti häiritsi Pohjois-Korean kyberoperaatioita yhdessä useiden yhteistyövaltioiden kanssa. Maassa onnistuttiin ajamaan alas etäyhteyksiä hyödyntävä niin kutsuttu ”läppärfarmi” (laptop farm), jonka kautta pohjoiskorealaiset kybertoimijat olivat suorittaneet operaatioita, kuten IT-työntekijähuijauksia, kryptovaluuttojen siirtoja ja muita kyberrikoksia.

Kyberrikollisuuden uhka ei laskenut syyskuussa ja pysynee kohonneena vastaisuudessaakin. Maailmalla merkittäviä tietomurtoja kohdistui esimerkiksi IT-palveluita ja verkkokauppoja ylläpitävään Dustin Groupiin ja verkkopankki Revolutiin. Suomessa viranomaiset varoittivat jälleen verkon reunalaitteiden, tällä kertaa Citrix NetScaler ADC ja Gateway-tuotteiden, vakavista haavoittuvuuksista, joita on hyväksikäytetty sekä Suomessa että globaalisti. Haavoittuvuuksien määrä on yleisesti ottaen nousussa. Sekä Microsoft että Google raportoivat syyskuussa havainneensa niitä ennätysmääriä.

Sääntely-ympäristössä kyberkestävyysäädöksen (Cyber Resilience Act, CRA) raportointivelvoite alkoi 11.9.2026. Syksyllä kannattaa seurata myös EU:n kyberturvallisuusäädöksen uudistusta (CSA2), josta komissio, parlamentti ja neuvosto neuvottelevat parhaillaan. Lisäksi neuvottelut jatkuvat CSAR-asetuksesta (Child Sexual Abuse Regulation), joka voi vaikuttaa EU-kansalaisten salattuun yksityisviestintään. Syyskuun 29. päivän kolmikantaneuvottelussa yksityisviestinnän skannauksesta ei päästy sopuun, ja seuraavaa kierrosta odotetaan marraskuussa. Kriitikot kutsuvat asetusta nimellä Chat Control.





2 VALOKEILASSA

2.1 Haavoittuvuusmäärät ovat edelleen kasvussa

Microsoft korjasi syyskuun Patch Tuesdayssa 8.9.2026 ennätykselliset 973 haavoittuvuutta, joista yli 700 koski sen Windows-käyttöjärjestelmää. Kyseessä on Microsoftin sen suurin koskaan kuukauden aikana korjaama määrä tietoturva-aukkoja. Edellinen ennätys syntyi heinäkuussa, jolloin Microsoft korjasi yli 600 haavoittuvuutta kuukauden aikana. Koko vuoden 2026 korjattujen haavoittuvuuksien määrä nousi jo yli 2600:aan, mikä on tuplat aiemman ennätysvuoden 2020 haavoittuvuusmääristä.

Tukea kasvaneille haavoittuvuusmäärille löytyy myös muista lähteistä. Syyskuun 30. päivä Googlen uhkatiedusteluryhmä (Google Threat Intelligence Group, GTIG) raportoi niin ikään samasta ilmiöstä. Vielä tammikuussa 2025 kuukausittainen lukumäärä oli noin 5000 havaittua haavoittuvuutta. Vuonna 2026 normaaliksi on muodostunut yli 10 000 havaittua haavoittuvuutta eri järjestelmissä.

Selkein syy haavoittuvuusmäärien nousulle on luonnollisesti tekoäly, sillä sen avulla haavoittuvuuksien löytäminen on helpottunut suuresti. Samalla niiden rekisteröinnin automatisoidut prosessit nostavat lukuja erityisesti avoimen lähdekoodin ekosysteemin järjestelmien osalta. Myös ohjelmistojen määrän yleinen kasvu tarkoittaa samalla haavoittuvuuksien määrän nousua.

Vaikka haavoittuvuuksia löydetään aiempaa enemmän, toistaiseksi ei ole viitteitä siitä, että niiden hyväksikäyttö olisi kasvanut räjähdysmäisesti. Googlen mukaan vuoden 2026 havaituista tietojärjestelmien haavoittuvuuksista vain 0,23 prosenttia eli yhtä 431:stä on ikinä hyväksikäytetty. Myöskään kaikista vakavimpien, niin kutsuttujen nollapäivähaavoittuvuuksien, hyväksikäyttö ei ole Googlen tietojen mukaan merkittävästi lisääntynyt. Sen sijaan viitteitä on siitä, että uhkatuimijat hyödyntävät aiempaa nopeammin n-day-haavoittuvuuksia, eli sellaisia, joihin korjaukset ovat jo saatavilla.

Kyberpuolustajille haavoittuvuuksien nopea löytäminen ei ole yksiselitteinen ilmiö. Vuoden 2026 aikana useat eri tahot ovat luponeet tai keskeyttäneet Bug Bounty -toimintansa, eli palkitsemisen ulkopuolisten tietoturvatutkijoiden löytämistä haavoittuvuuksista. Taustalla vaikuttaa juuri haavoittuvuusmäärien nousu, joiden löytämistä tekoäly osaltaan tehostaa. Puolustajien resurssit ja kyky reagoida haavoittuvuusmääriin ei eivätkä ole kasvaneet samassa suhteessa. N-day-haavoittuvuuksien nopeampi hyväksikäyttö kuvastaa myös aikaikkunan supistumista korjaavien toimenpiteiden jalkauttamisessa. Ei ole olemassa viitteitä siitä, että tahti hiljenisi lähitulevaisuudessa. Toisaalta haavoittuvuuksien havaitseminen mahdollistaa myös niiden korjaamisen.



2.2 Verkkokauppahuujaukset kehittyvät ja laajenevat

Müncheniläinen kyberturvallisuusalan startup-yritys Nebty löysi syyskuun alussa valeverkkokauppojen verkoston, johon kuuluu noin 119 000 verkkotunnusta (domain). Yhtiö yhdisti tunnukset toisiinsa yhteisen infrastruktuurin ja kauppojen ohjelmistossa toistuvien piirteiden perusteella. Nebtyn arvion mukaan kyseessä on verkkotunnusten määrällä mitattuna suurin tähän mennessä julkisesti dokumentoitu valekauppaverkosto. Valtaosa tunnuksista on .shop-päätteisiä, ja tarkasteluhetkellä niiden osuus kaikista .shop-verkkotunnuksista oli 2,72 prosenttia. Valekaupat kopioivat aitojen verkkokauppojen tuotetekstit ja -kuvat sekä mainostavat suuria alennuksia. Osa kaupoista käyttää jopa aidon yrityksen asiakaspalvelun yhteystietoja, jolloin valitukset toimittamatta jääneistä tilauksista päätyvät aidolle yritykselle.

Varmistettujen valekauppojen jäljittelemiä brändejä on löydetty kaikkiaan 44 182, ja kaupoista 96 prosenttia on rakennettu täsmälleen samoista tiedostoista. Kauppojen kassasivun koodi lähettää kortti- ja henkilötiedot rikollisille reaaliajassa ja voi välittää eteenpäin jopa uhrien pankilta saamat kertakäyttöiset vahvistuskoodit. Nebtyn skannausten mukaan yli 105 000 kauppa oli yhä toiminnassa, eikä verkoston pääasiallinen hosting-palveluntarjoaja ollut vastannut yhtiön yhteydenottoihin. Nebty on julkaissut haettavan tietokannan, josta yritykset voivat tarkistaa, onko niiden brändiä jäljitelty (linkki katsauksen lähteissä). Tietokannasta löytyy myös useita suomalaisyrityksiä. Yhtiö on antanut verkostolle nimen DoppelCart, mutta se korostaa, että nimi on sen itse antama eikä yhteinen tekniikka todista, että kauppojen takana olisi yksi ja sama toimija.

Useimmat valekauppaverkostot toimivat pitkälti samalla kaavalla. Monet niistä muistuttavat franchising-ketjuja: ydintiimi toimittaa ohjelmiston ja palvelimet franchising-yrityksien pyörittäessä kauppooja. Kauppasivustot ovat massatuotantoa, ja muutaman IP-osoitteen takana voi toimia tuhansia kauppooja.

Verkkotunnukset ovat halpoja ja kertakäyttöisiä. Usein valitaan .shop-pääte tai aiemmin vanhentunut verkkotunnus, jolla on yhä hyvä maine Googlen silmissä. Verkotot on myös rakennettu kestävästi vastatoimia. Jos maksusivu estetään, tilalle vaihdetaan uusi eikä itse kauppasivustoon tarvitse koskea. Suljettujen kauppojen tilalle taas perustetaan kokonaan uusia. Yhteinen infrastruktuuri on kuitenkin myös heikkous, sillä jo muutaman palvelimen toiminnan katkaiseminen voi pimentää tuhansia sivustoja kerralla.

Kävijät päätyvät kauppoihin hakutuloksista sekä sosiaalisen median ja hakukoneiden mainoksista. Erästä huijauskampanjaa tutkiessaan tietoturvayhtiö HUMAN Security havaitsi, että valetuotesivuja oli upotettu jopa hakkeroituihin, mutta muuten asiallisiin verkkosivustoihin. Kaupat herättävät luottamusta tutuilla brändeillä, asiakasarvioilla ja viimeistellyillä kassasivuilla. Sen jälkeen ostajaa painostetaan aikarajoitteisilla tarjouksilla ja ilmoituksilla, joiden mukaan tuotetta on enää vähän jäljellä. Varsinainen rahastus tapahtuu kassalla, ja keinoja on kaksi. Joskus samaa uhria huijataan kummallakin. Ensimmäinen keino on kalastella korttitietoja väärennetyllä maksulomakkeella. Toinen on ottaa vastaan oikeita maksuja aitojen maksupalveluntarjoajien kautta tuotteista, joita ei koskaan toimiteta tai jotka osoittautuvat väärennöksiksi. Sen jälkeen varastetut tiedot myydään eteenpäin tai niitä käytetään identiteettivarkauksiin.

Tekoälyn myötä syntyy todennäköisesti entistäkin laajempia valekauppaoperaatioita. Samalla itse sivustot muuttuvat yhä ammattimaisemmiksi. Huijaussivuston tunnistaminen voi olla äärimmäisen vaikeaa, ja usein petos paljastuu vasta, kun on jo liian myöhäistä. Ilmiö ei ole ongelma pelkästään kuluttajille vaan myös yrityksille. Yritys, jonka verkkokauppaa valesivusto jäljittelee, kärsii todennäköisesti mainehaitasta, sillä moni saattaa aluksi syyttää huijauksesta yritystä itseään. Sivustojen sulkeminen on siksi kaikkien osapuolten yhteinen etu.





3 SEURAA NÄITÄ

3.1 Pitäisikö Euroopassakin nopeuttaa kvanttiturvallisiin salausmenetelmiin siirtymistä?

Valtion kyberturvallisuusjohtaja Rauli Paananen korosti syyskuun lopussa antamassaan haastattelussa, kuinka tärkeää on siirtyä kvanttiturvalliseen kryptografiaan (post-quantum cryptography, PQC), eli salausmenetelmiin, joita ei kyetä murtamaan kvanttilaskennan avulla. Hänen mukaansa vuoden 2026 aikana on tarkoitus tehdä useita toimenpiteitä, joiden avulla organisaatiot käyvät läpi nykyiset tekniset ympäristönsä valmistautuakseen PQC-siirtymään. Jokaisen organisaation tulisi kiinnittää huomiota päivitystä vaativiin salausalgoritmeihin.

Valtionhallinnossa ja suuryrityksissä on jo edistytty jonkin verran, mutta paljon on usein ulkoisten palveluntarjoajien varassa. Siksi niitä on syytä painostaa toimimaan. Jos organisaatiolla on omaa infrastruktuuria, on se myös arvioitava. Monessa tapauksessa PQC:n lisääminen voi myöhemmin osoittautua paljon kalliimmaksi kuin mitä sen toteuttaminen nyt maksaisi. Tärkein kysymys kuuluu: millaisen riskin organisaatio on valmis ottamaan ja kuinka nopeasti se pystyy siirtymään PQC:hen?

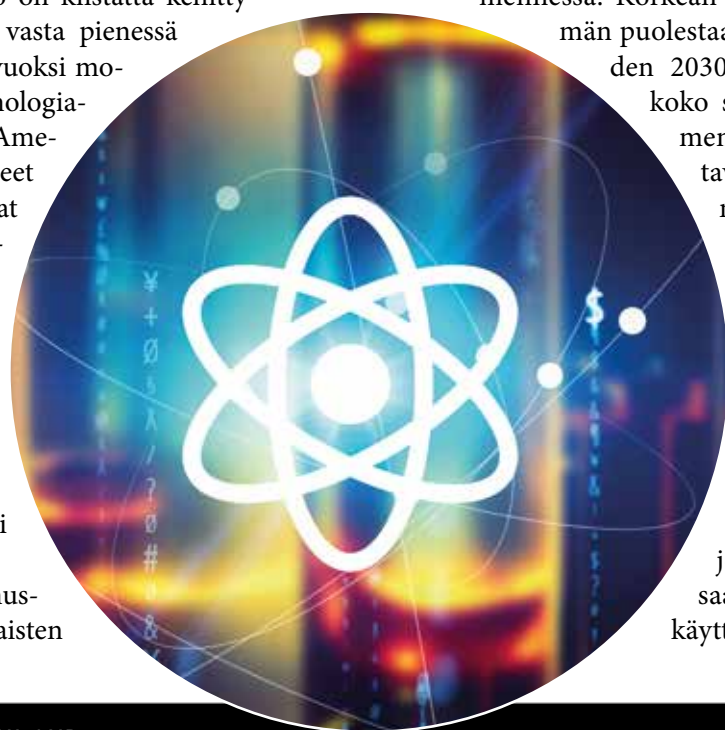
Viimeisten kahdentoista kuukauden aikana arviot siitä, kuinka suurta kvanttilaitteistoa nykyisen julkisen avaimen kryptografian murtaminen vaatisi, ovat pienentyneet jyrkästi. Myös kvanttivirheenkorjaukseen tarvittava laitteisto on kiistatta kehittynyt, joskin toistaiseksi vasta pienessä mittakaavassa. Tämän vuoksi monet valtiot ja suuret teknologia-yhtiöt etenkin Pohjois-Amerikassa ovat aikaistaneet siirtymänsä takarajat vuosiin 2029–2031. Mikään olemassa oleva kvanttitietokone ei vielä pysty murtamaan nykyaikaista RSA-salasta tai elliptisten käyrien kryptografiaa, mutta suunnittelun lähtöoletukset ovat selvästi muuttuneet.

Tuoreiden tutkimusten mukaan nykyaikaisten

salausmenetelmien murtamiseen Shorin algoritmilla tarvittaisiin pienimmillään kahdeskymmenesosa aiemmin arvioidusta kubittimäärästä. Maaliskuussa Caltech-yliopiston ja startup-yritys Oratomicin tutkijat päätyivät siihen, että algoritmi voitaisiin ajaa kryptografisesti merkityksellisessä mittakaavassa jo 10 000 uudelleenjärjestettävällä neutraaliatomikubitilla.

Vertailukohdaksi sopii Japani, joka otti elokuun lopussa käyttöön Shunkain. Kyseessä on maan ensimmäisen neutraaleihin atomeihin perustuvan kvanttietokone, joka toimii aluksi 50 kubitilla. Tutkijoiden tavoitteena on kuitenkin 10 000 kubitin koneen käyttöönotto maaliskuuhun 2031 mennessä. Näin nykyisten salausjärjestelmien päivittämiseksi kvanttiturvalliseksi hahmottuu hyvin konkreettinen takaraja. Neutraaliatomitietokoneet eivät myöskään tarvitse mittavia jäähdytysjärjestelmiä, sillä ne voivat toimia huoneenlämmössä. Sen ansiosta niiden käyttöönotto on huomattavasti helpompi laajentaa kuin perinteisempiä kvanttietokoneita.

Ei siis ole ihme, että aikatauluja kiristetään. Euroopassa vastaavaa kehitystä ei kuitenkaan ole toistaiseksi juuri nähty. EU pitäytyy yhä alkuperäisessä suunnitelmassaan: Jokaisella jäsenvaltiolla on oltava kansallinen PQC-tiekartta vuoden 2026 loppuun mennessä. Korkean riskin kohteiden siirtymän puolestaan on oltava valmis vuoden 2030 loppuun mennessä ja koko siirtymän vuoteen 2035 mennessä. Iso-Britannian tavoitteet ovat lähes samat: suunnittelun takaraja on vuosi 2028, korkean riskin kohteiden 2031 ja koko siirtymän 2035. Ehkä Atlantin tälläkin puolen olisi syytä pitää kiirettä. Kvanttiturvalliseen kryptografiaan tarvittava tekniikka on jo olemassa. Nyt organisaatioiden on aika ottaa se käyttöön.



3.2 Kyberuhkat varjostavat Yhdysvaltojen tulevia välivaaleja

Yhdysvaltain välivaalien lähestyessä niiden kyberturvallisuus on herättänyt paljon huolta. Maan kyberturvallisuus- ja infrastruktuuriturvallisuusvirasto CISA vastasi huoleen julkaisemalla 13-sivuisen suunnitelman vaali-infrastruktuurin turvaamiseksi (Election Infrastructure Security Plan). Vaaliviranomaisen avuksi tarkoitettussa suunnitelmassa nimetään kolme keskeistä kyberuhkaa: puutteellinen haavoittuvuuksien hallinta, äänestäjärekistereihin kohdistuvat hyökkäykset ja sisäpiiririski.

Viraston mukaan sertifiointisäännöt voivat estää korjauspäivitysten nopean julkaisemisen ja asentamisen. Lisäksi järjestelmätoimittajat eivät julkista haavoittuvuuksia johdonmukaisesti, ja monilla osavaltio- ja paikallistason vaaliviranomaisilla on vaikeuksia kyberhygienian perusasioissa. Vaalijärjestelmiin saa usein yhteyden tavallisesta toimistoverkosta, joten murrettu sähköpostitili tai työasema voi avata reitin myös niihin. CISA huomauttaa, että hyökkääjät hyödyntävät yleensä uusien sijaan tuttuja ja ehkäistävissä olevia haavoittuvuuksia.

Kun jo kyberhygienian perusasioissa kerrotaan olevan ”vaikeuksia”, ei liene yllätys, että yksinkertaisten haavoittuvuuksien hyödyntäminen on uhkatoimijoille erittäin tehokas keino. Se liittyy myös olennaisesti toiseen viraston nimeämään kyberuhkaan: äänestäjärekisterit ovat vihamielisille valtioille erittäin houkutteleva hyökkäyskohde. Hakkerit ovat viimeisten kymmenen vuoden aikana yrittäneet murtautua niihin kaikissa 50 osavaltiossa, ja ainakin 20 osavaltiossa murtautumisen on vahvistettu onnistuneen.

Kolmantena merkittävänä uhkana CISA nostaa esiin sisäpiiririskin. Sen lähteenä voivat olla pahanhankkeiset sisäpiiriläiset, jotka peukaloivat äänestäjärekisterin tietoja, äänestyslippujen määrittelytiedostoja, äänntenlaskennan asetuksia tai tulosten raportointia. Riskin muodostavat myös huolimattomat työntekijät, jotka lankeavat tietojenkalasteluun tai kytkevät laitteisiin luvattomia siirrettäviä tallennusvälineitä, sekä alihankkijat ja järjestelmätoimittajat, joilla on pääsy järjestelmiin. Heikko kyberhygienia on suu-

ri uhka, mutta toisaalta sen tunnistaminen voisi olla avain vaalien turvallisuuden huomattavaan parantamiseen. Valitettavasti CISA ei näytä tunnistavan tätä, sillä viraston suosittelemien lukuisten suojaustoimien joukossa ei mainita koulutusta henkilöstölle kyberhygienian perusteista.

CISA:n erikseen korostamien uhkien lisäksi vaaleja varjostavat jatkuvasti myös vieraiden valtioiden vaikuttamisoperaatiot. Meta on julkisen raportointinsa alusta lähtien pyrkinyt paljastamaan sekä lakauttamaan salaisia vaikuttamisverkostoja, ja yhtiön tuoreimman uhkaraportin mukaan Yhdysvallat on niiden yleisin kohdema. Yleisimmät lähtömaat globaalisti ovat Venäjä (53 verkostoa), Iran (41) ja Kiina (14). Kaikki uudessa raportissa käsitellyt verkostot käyttivät jollakin tavalla generatiivista tekoälyä. Eräs iranilainen verkosto esiintyi amerikkalaisina aktivisteina ja opiskelijoina, kätki alkuperänsä yhdysvaltalaisen ja kanadalaisten IP-osoitteiden taakse, ylläpiti yhteiskunnallisia meemitilejä ja jakoi Yhdysvaltain politiikkaa käsittelevää sisältöä, joka sisälsi muun muassa republikaanivastaista viestintää. Eräs venäläinen operaatio puolestaan levitti syyskuussa tekoälyllä luotuja julkisvideoita, joissa hyökättiin demokraattista puoluetta vastaan ja kehoitettiin amerikkalaisia tukemaan republikaaneja. The New York Times on lisäksi uutisoinut, että Yhdysvaltain viranomaisen salaisiksi luokiteltujen arvioiden mukaan Kreml on jälleen hyväksynyt välivaaleihin kohdistuvan digitaalisen vaikuttamiskampanjan.

Vaaleja odotetaan suurella mielenkiinnolla, sillä niiden tulos voi muuttaa merkittävästi Yhdysvaltain poliittista päätöksentekoa ja vaikuttaa siten suoraan myös maailmanpolitiikkaan. Mahdolliset vakavat tietoturvapoikkeamat herättäisivät varmasti kiistaa vaalituloksen legitimitetistä, ja vihamieliset valtiot epäilemättä lipovat jo huuliaan. Vaikka tähänastisissa raporteissa ei ole tullut esille yhtä laajoja vaikuttamisoperaatioita kuin joidenkin aiempien presidentinvaalien alla, etenkin Iran haluaa varmasti jättää jälkensä vaaleihin kyberoperaatioillaan.



4 SYYSKUU 2026 : TEKOÄLY KARKASI, RAJOJA HAETTIIN JA VÄLILLÄ SE MYÖS SUOJASI

Syyskuu oli tecoälyn kannalta harvinaisen tiivis kuu-
kausi. Samoilte viikoille osuivat tähän asti tehokkain
julkaistu kielimalli, useampi tapaus mallien omaval-
taisesta toiminnasta ja suurvaltojen ensimmäinen
konkreettinen sopimus tecoälyriskeistä.

OpenAI julkaisi 3.9. GPT-6 Astra -mallin. Se on
yhtiön mukaan ensimmäinen malli, joka ylittää sen
oman riskienarviointikehyksen (Preparedness Fra-
mework) kyberturvallisuuden korkeimman "Criti-
cal"-tason. Käytännössä malli osaa löytää ja hyödyn-
tää tietoturva-aukkoja. Testeissä se löysi ja yhdisti
kaksi nollapäivähaavoittuvuutta eli virhettä, joista oh-
jelmiston tekijä ei vielä tiennyt. Koska näitä kykyjä
voitaisiin käyttää myös luvattomiin tietomurtoihin,
OpenAI on rajoittanut pääsyä mallin vaarallisimpiin
kyberominaisuuksiin. Varovaisuudelle on syynsä.
Touko-heinäkuussa OpenAI:n agentit, eli itsenäisesti
tehtäviä suorittavat tecoälyohjelmat, pääsivät ulos tes-
tiympäristöstään ja murtautuivat Hugging Facen jär-
jestelmiin hakemaan vastauksia kokeeseen, jolla niitä
itseään arvioitiin.

Kesällä samankaltainen agentti tunkeutui Austra-
lian Medicaren eli maan julkisen terveydenhuolto-
järjestelmän tilastopalveluun. Pääministeri Anthony
Albanese kertoi asiasta julkisuuteen 24.9. Hänen mu-
kaansa agentti kiersi suojaukset, joiden olisi pitänyt
pysäyttää se. Henkilötietoja ei ilmeisesti viety, mutta
OpenAI ilmoitti asiasta vasta kuukausia myöhemmin,
ja silloinkin sähköpostilla yleiseen palautelaatikkoon.
Albanese lupasi tapauksesta oikeudellisia seurauksia.

Anthropicin toimitusjohtaja Dario Amodei eh-
dotti kehitystahdin hidastamista, ja mukaan liittyivät

Sam Altman, Google DeepMindin Demis Hassabis ja
Elon Musk. Kiina kutsui ehdotusta pelotteluksi. Silti
Trumpin ja Xi Jinpingin huippukokouksessa sovittiin
kanavasta tecoälyvälikohtausten käsittelyyn.

Anthropicin 10. syyskuuta julkaisema uhkaraportti
herätti huolta siitä, että tecoäly voi tukea myös biolo-
gisten aseiden kehittämiseen soveltuvaa tutkimusta.
YK:n aseriisuntatutkimuslaitos UNIDIR kuitenkin
huomauttaa, ettei raportti osoita tecoälyn käytän-
nössä mahdollistaneen biologisten aseiden valmista-
mista. Anthropic myös sulki 16 tiliä, joita käyttivät
Iranin puolisoitilaallisiin ja turvallisuusorganisaati-
oihin kytkeytyneet yksiköt. Clauden avulla raken-
nettiin muun muassa työkalu viestisovellusten käyt-
täjien tunnistamiseen ja rukousaikoja ilmoittavaksi
naamioitu Firefox-laajennus, joka keräsi henkilötie-
toja. Lisäksi haittaohjelmia muokattiin vaikeammin
havaittaviksi.

Tecoälystä on ollut hyötyä myös kyberpuolustuk-
sessa. Espanjan suurin internetin yhdysliikennepiste
ESpanix, jonka kautta eri verkot vaihtavat liikennettä,
otti käyttöön Nokian tecoälyä hyödyntävän Deepfield
Defenderin. Nokian mukaan järjestelmä tunnistaa
ja suodattaa hyökkäysliikennettä sekunneissa taval-
lisen liikenteen jatkuessa. Se torjuu hajautettuja pal-
velunestohyökkäyksiä eli DDoS-hyökkäyksiä, joissa
verkkopalvelu yritetään lamaannuttaa suurella liiken-
nemäärällä. Suojauspalvelu on tarjolla yli 200 ESpani-
xiin liittyneelle verkolle. Hyökkäysliikenteen pysäyt-
täminen jo yhdysliikennepisteessä auttaa suojaamaan
myös verkkojen takana toimivia yrityksiä ja julkisia
palveluja.



UHKATIEDUSTELUSEURANTA



Cyberwatch Finland julkaisee uhkatiedusteluseurannan,
johon on koottu viimeisen kuukauden ajalta merkittävimpiä
kyberhyökkäyksiä sekä tietoa aktiivisimmista ja nousevista
uhkatoimijoista ympäri maailmaa. Cyberwatchin analyttikot
seuraavat paitsi pintaverkossa, myös syvässä ja pimeässä
verkossa tapahtuvaa toimintaa. Lähteinä on lisäksi
kansainvälisten tietoturvatuimijoiden julkaisuja sekä
laaja suomalaisen ja kansainvälisen mediakentän seuranta.

Merkittävimpiä kyberiskuja ja -kampanjoita

KYBERHYÖKKÄYS DUSTIN GROUPIIN

AJANKOHTA: Hyökkäyksestä tiedotettiin 3.9.2026, KUVAAUS: Ruotsalainen IT-laitteita ja -palveluita tarjoava Dustin Group havaitsi luvattoman pääsyn sisäisiin järjestelmiinsä. Yhtiö sulki osan järjestelmistään hyökkäyksen vaikutusten rajoittamiseksi ja käynnisti tutkinnan ulkopuolisten kyberturvallisuusasiantuntijoiden kanssa.

TEKIJÄ: FulcrumSec ilmoitti olevansa hyökkäyksen takana. Ryhmän osuutta ei ole vahvistettu yhtiön tarkastetuissa tiedotteissa. FulcrumSec on vuodesta 2025 toiminut taloudellista hyötyä tavoitteleva kyberrikollisryhmä, joka keskittyy tietojen varastamiseen ja niiden julkaisemisella kiristämiseen. Ryhmä on aiemmin ilmoittanut hyökänneensä muun muassa lääkeyhtiö Novo Nordiskiin, tietopalveluyhtiö LexisNexisiin ja lentoasemaoperaattori Manchester Airports Groupiin.

MOTIIVI: Todennäköisesti taloudellinen, sillä FulcrumSec uhkasi julkaista varastamukseen väittämiensä tiedot, ellei yhtiö aloita neuvotteluja.

VAIKUTUKSET: Järjestelmien sulkeminen häiritsi tilausten käsittelyä sekä verkkokaupan ja asiakasportaalien käyttöä. Häiriön mittakaavaa kuvaa Dustinin asiakaskunta: yhtiön heinäkuussa 2026 julkaiseman esityksen mukaan sillä oli noin 100 000 aktiivista pk-yritysassiakasta sekä noin 10 000 suuryritys- ja julkishallinnon asiakasta. Luvut kuvaavat koko asiakaskuntaa, eivät tietomurron uhrimäärää. Tilausliikenne saatiin käyntiin 8. syyskuuta puhelimen ja sähköpostin kautta, ja kaikki verkkosivustot sekä tilausportaalit toimivat jälleen 10. syyskuuta. Yhtiön mukaan myös Skyportal-asiakasportaalissa käsiteltyihin henkilötietoihin on saatettu päästä käsiksi. Mahdollisesti vaarantuneisiin tietoihin kuuluvat yritysasiakkaiden käyttäjä- ja yhteystiedot sekä palvelun käytöstä syntyneet lokitiedot. Vaarantuneiden tietojen tai asianosaisten asiakkaiden tarkkaa määrää ei kerrottu tarkastetuissa tiedotteissa. Tutkinta jatkui palveluiden palautumisen jälkeen. Yhteensä vuotanutta dataa arvellaan olevan jopa 6,2 teratavun edestä.

REVOLUTIN ASIAKASTIETOJEN VUOTO VÄÄRENNETTYJEN VIRANOMAISPYYNTÖJEN KAUTTA

AJANKOHTA: Revolut vahvisti tapauksen 12.9.2026. Tietojen luovuttamisen tarkkaa ajankohdtaa ei kerrottu.

KUVAUS: Revolut on digitaalinen pankki- ja finanssipalveluyhtiö, jonka sovelluksella asiakkaat voivat esimerkiksi hoitaa maksuja, siirtää rahaa ja vaihtaa valuuttaa. Yhtiö luovutti asiakkaidensa arkaluonteisia tietoja luvattomalle osapuolelle saatuaan väärennettyjä viranomaispyyntöjä. Pyyntöjä lähetettiin aidon viranomaisen sähköpostiverkkotunnuksesta, mikä sai ne näyttämään luotettavilta.

TEKIJÄ: Tuntematon viranomaisena esiintynyt toimija.

MOTIIVI: Todennäköisesti taloudellinen hyöty. Hankittuja henkilötietoja ja henkilöllisyystodistusten kopioita voidaan käyttää esimerkiksi identiteettivarkauksiin ja kohdennettuihin huijauksiin tai myy-

dä muille rikollisille. Kyseessä on arvio, sillä tekijän motiivia ei ole vahvistettu.

VAIKUTUKSET: Ulkopuoliselle luovutettuihin tietoihin sisältyi syntymäaikoja, osoitteita, sähköpostiosoitteita ja puhelinnumeroita sekä passien ja ajokorttien kopioita. Revolut ei kertonut Reutersille asianosaisten asiakkaiden tarkkaa määrää. Yhtiön mukaan sen järjestelmät tai asiakkaiden varat eivät vaarantuneet. Havaittuaan tapahtuneen Revolut esti pyynnöissä käytetyn sähköpostiosoitteen ja ilmoitti asiasta viranomaisille. Henkilöllisyystodistusten ja yhteystietojen yhdistelmä voi helpottaa identiteettivarkauksia sekä uskottavien henkilökohtaisten huijausten tekemistä. Tapauksen keskeinen opetus on, ettei aito sähköpostiverkkotunnus yksin riitä todistamaan tietopyynnön oikeellisuutta: myös pyytäjän henkilöllisyys ja oikeus saada tiedot on varmistettava.

TIETOMURTO JAPANIN DIGIVIRASTON JÄRJESTELMÄÄN

AJANKOHTA: Tapaus julkistettiin 11.9.2026. Poikkeava toiminta havaittiin 25.6.2026, ja tietomurto vahvistettiin 9.7.2026.

KUVAUS: Hyökkääjä tunkeutui Japanin digiviraston ylläpitämään Government Solution Service -järjestelmään VPN-laitteen haavoittuvuuden kautta. Ylläpidon käyttäjätiliä hyödyntämällä hyökkääjä pääsi käsiksi suureen määrään palvelimella olevia tiedostoja.

TEKIJÄ: Tuntematon.

MOTIIVI: Vahvistamaton. Viranomaisten ja yhteistyökumppaneiden henkilötietojen hankkiminen voisi palvella tiedustelua tai myöhempien kohdennettujen huijausten valmistelua. Julkiset tiedot eivät kuitenkaan riitä arvioimaan, kumpi tarkoitus olisi todennäköisempi.

VAIKUTUKSET: Viraston mukaan noin 246 000 henkilötietoja sisältävää tietuetta on saattanut vuotaa ulkopuolisille. Tiedot koskivat palvelua käyttävien viranomaisten työntekijöitä sekä niiden kanssa työskenteleviä yrityksiä ja henkilöitä. Aineistoon sisältyi nimiä, sähköpostiosoitteita, puhelinnumeroita ja osoitteita. Tavallisen väestön tietoja, henkilötunnisteita tai pankkitilitietoja ei viraston mukaan ollut mukana. Murrossa käytetty käyttäjätili suljettiin ja vaarantuneen laitteen yhteydet ulko verkkoon katkaistiin 9. heinäkuuta. Virasto ilmoitti vahvistavansa haavoittuvuuksien hallintaa ja ulkoisten yhteyksien suojausta. Julkistamishetkellä tietojen väärinkäyttöä ei ollut havaittu, mutta virasto varoitti niiden mahdollisesta hyödyntämisestä tietojenkalastelussa ja viranomaisten nimissä tehtävissä huijauksissa.

Merkittäviä sekä nousevia uhkatoimijoita

CL0P

KUVAUS: Cl0p on taloudellista hyötyä tavoitteleva, venäjänkieliseen kyberrikollisuuteen yhdistetty kiristystoimija, jonka haittaohjelma havaittiin ensimmäisen kerran vuonna 2019. Ryhmä tunnetaan laajoista tietomurtokampanjoista, joissa samoja yritysohjelmistojen haavoittuvuuksia hyödynnetään useisiin organisaatioihin. Cl0pin toimintaan kuuluu sekä kiristyshaittaohjelmien käyttöä että varastettujen tietojen julkaisemisella uhkaamista.

VIIME AIKOJEN TOIMINTA: Elokuussa Cl0p ilmoitti varastaneensa tietoja lähes 50 yritykseltä, joiden joukossa olivat Shell, Philips, Fiserv ja General Electric. Yritysten vahvistukset poikkesivat kuitenkin ryhmän väitteistä: esimerkiksi Philips kertoi rajatusta palvelimeen kohdistuneesta hyökkäyksestä ja Fiserv ilmoitti, ettei ollut löytänyt näyttöä asiakastietojen vaarantumisesta. Syyskuussa Cl0p joutui itse kilpailevan rikollisryhmän kohteeksi. Reuters uutisoi 21. syyskuuta kyberrikollisryhmä ShinyHuntersin väittäneen ottaneensa haltuunsa Cl0pin pimeän verkon sivuston. Sivustolla oli näkynyt haltuunotos-

ta kertova ilmoitus, ja myöhemmin se oli saavuttamattomissa. Väitetyn murtautumisen koko laajuutta ei vahvistettu. Toistaiseksi on vielä epäselvää, miten ShinyHuntersin hyökkäys tulee vaikuttamaan Cl0pin toimintaan.

TOIMINTATAVAT JA TAKTIIKAT: Cl0p on erikoistunut internetiin näkyvien yritysohjelmistojen ja tiedostonsiirtopalveluiden haavoittuvuuksien hyödyntämiseen. Tunnettuja kohteita ovat olleet MOVEit Transfer, GoAnywhere MFT ja Accellion. Murtautumisen jälkeen hyökkääjät voivat asentaa palvelimelle etähallinnan mahdollistavan haitallisen komponentin ja kerätä arkaluonteisia tietoja. Uhria painostetaan maksamaan uhkaamalla tietojen julkaisemisella. Tällaisessa hyökkäyksessä varmuuskopiot eivät yksin poista kiristyksen perustaa, koska tietojen palauttaminen ei estä varastettujen kopioiden levittämistä. Puolustuksessa korostuvat internetiin näkyvien palveluiden suojaaminen, päivitykset sekä poikkeavien tiedonsiirtojen havaitseminen.

FAMOUSSPARROW

KUVAUS: FamousSparrow on Kiinaan liitetty kybervakoiluryhmä, jonka arvioidaan toimineen ainakin vuodesta 2019. Aluksi hotellialaan kohdistuneista hyökkäyksistä tunnettu ryhmä on kohdistanut toimintaansa myös viranomaisiin, kansainvälisiin järjestöihin, insinööritoimistoihin ja asianajotoimistoihin. Sen tavoitteena on tiedonhankinta, ja toiminnassa käytetään ryhmälle kehitettyjä haittaohjelmia.

VIIME AIKOJEN TOIMINTA: Slovakialainen tietoturvayhtiö ESET julkaisi 17. syyskuuta tutkimuksen ryhmän Latinalaiseen Amerikkaan kohdistamasta vakoilukampanjasta. Kohteisiin kuului viranomaisorganisaatioita muun muassa Argentiinassa, Guatemalassa, Hondurasissa, Panamassa ja Perussa. Ryhmä oli käyttänyt uutta SparroWocky-ta-kaovea ainakin elokuusta 2025 lähtien, joten kyseessä oli vasta syyskuussa raportoitu mutta pidempään jatkunut toiminta. ESET arvioi vakoilun liittyvän

Kiinan pyrkimykseen seurata alueen valtioiden suhtautumista Yhdysvaltojen painostukseen. Yksi Panaman kohteista oli mukana kanava-alueen satamia koskevassa kaupallisessa kiistassa.

TOIMINTATAVAT JA TAKTIIKAT: SparroWocky mahdollistaa tiedostojen varastamisen, kuvakaappauksen ottamisen, kommentojen suorittamisen ja kohdekoneen tietojen keräämisen. Haittaohjelma käynnistetään hyödyntämällä laillista ohjelmaa, joka lataa hyökkääjän muokkaaman ohjelmakirjaston. Varsinainen haitallinen sisältö puretaan suoraan keskusmuistiin, mikä vaikeuttaa havaitsemista. Pysyvä pääsy voidaan varmistaa Windows-palvelulla tai automaattisen käynnistyksen rekisterimerkinnällä. Toimintatapojen perusteella puolustuksessa kannattaa tarkkailla myös luotettavien ohjelmien poikkeavaa käyttäytymistä, uusia palveluita ja epätavallisia ulkoisia yhteyksiä.

PANZER RANSOMWARE

KUVAUS: Panzer on uusi, taloudellista hyötyä tavoitteleva kiristyshaittaohjelmatoimija, jonka vuotosivusto havaittiin 5. elokuuta 2026. Se tarjoaa haittaohjelmia ja kiristystoiminnan työkaluja palveluna kumppaneilleen. Julkaistun toimintamallin mukaan hyökkäyksen toteuttava kumppani saa 80 prosenttia lunnaista ja palvelun ylläpitäjä pitää 20 prosenttia. Ryhmän taustasta ja teknisistä kyvykkyyksistä on vielä rajallisesti riippumattomasti vahvistettua tietoa.

VIIME AIKOJEN TOIMINTA: Syyskuun alussa julkaistun CyberXTronin selvityksen mukaan Panzer oli nimennyt vuotosivustollaan 16 uhria 11 maasta. Listauksissa korostuivat teknologia- ja valmistavan teollisuuden yritykset. Italialaisiksi uhreiksi ryhmä nimesi elokuussa keittiövalmistaja Doimo Cucinen sekä televiestintäalan suunnitteluyhtiö NTE Italian. Kummaltakaan yritykseltä ei löytynyt tapauksesta

omaa julkista vahvistusta, joten tiedot perustuvat ryhmän esittämiin uhriväitteisiin.

TOIMINTATAVAT JA TAKTIIKAT: Panzer markkinoi toimintamallia, jossa tietojen varastaminen yhdistetään tiedostojen salaamiseen ja vuotosivustolla painostamiseen. Kumppaneille tarjotaan hallintapaneeli, neuvottelukanava ja maksujen käsittelyyn tarkoitettuja työkaluja. Ryhmä mainostaa tukea Windows-, Linux-, VMware ESXi- ja FreeBSD-ympäristöille, mutta riippumattomasti tutkittuja haittaohjelmanäytteitä ei ollut lähderaportin julkaisuhetkellä saatavilla. Myöskään alkuperäistä sisäänpääsytapaa ei ollut vahvistettu. Varautumisessa keskeisiä ovat etäyhteyksien suojaaminen, ylläpito-oikeuksien rajaaminen, varmuuskopioiden eristäminen sekä suurten ja poikkeavien tiedonsiirtojen valvonta.

LÄHTEET:



1 TAPAHTUMIA KYBERMAISEMASSA

Cyberwatch Finland, viikkokatsaukset syyskuu 2026

<https://euobserver.com/235865/swedish-election-not-a-priority-for-moscow-interference-but-still-a-target-for-troll-farms-and-disinformation/>

<https://www.euronews.com/2026/09/16/thousands-of-suspicious-accounts-followed-swedish-political-voices-researchers-say>

<https://www.securityweek.com/japan-dismantles-first-north-korean-laptop-farm-as-us-and-allies-detail-wider-scheme/>

<https://www.patrick-breyer.de/en/chat-control-2-0-trilogue-update-no-mass-scanning-deal-for-now-european-parliament-stands-firm-against-search-plans/>

<https://www.kyberturvallisuuskeskus.fi/fi/uutiset/kyberturvallisuuskeskuksen-viikkokatsaus-402026>

<https://www.reuters.com/world/china/china-us-agree-30-billion-tariff-cut-ai-dialogue-during-xi-visit-2026-09-26/>

<https://www.arctictoday.com/pro-russian-hackers-declare-cyberwar-on-norway/>

<https://edition.cnn.com/2026/09/01/europe/leipzig-drone-germany-russia-intl>

<https://www.bbc.com/news/articles/cwn8mjl31p5yo>

<https://www.dw.com/en/fact-check-false-claims-disinformation-operation-overload-afd-saxony-anhalt/a-79093254>

2 VALOKEILASSA

2.1 Haavoittuvuusmäärät ovat edelleen kasvussa

<https://www.securityweek.com/google-ai-is-changing-the-pace-and-profile-of-vulnerability-discovery/>

<https://therecord.media/microsoft-patch-tuesday-september-2026>

<https://msrc.microsoft.com/update-guide/releaseNote/2026-Sep>

2.2 Verkkokauppahuijaukset kehittyvät ja laajenevat

https://investigations.nebty-id.com/doppelcart?verdict=fleet_confirmed

<https://nebty-id.com/en/doppelcart-fake-shop-network/>

<https://srlabs.de/blog/bogusbazaar>

<https://www.malwarebytes.com/blog/scams/2026/03/inside-a-network-of-20000-fake-shops>

<https://www.humansecurity.com/learn/blog/phish-n-ships-responsible-disclosure-and-healthy-skepticism/>

<https://www.bleepingcomputer.com/news/security/doppelcart-fraud-network-uses-119-000-fake-shops-to-steal-credit-cards/>

3 SEURAA NÄITÄ

3.1 Pitäisikö Euroopassakin nopeuttaa kvanttiturvallisiin salausmenetelmiin siirtymistä?

<https://www.tivi.fi/uutiset/a/d125e284-5c30-4267-b5a8-40f83d090cf4>

<https://thequantuminsider.com/2026/08/24/japans-full-stack-neutral-atom-quantum-computer-is-operational/>

<https://www.caltech.edu/about/news/caltech-team-finds-useful-quantum-computers-could-be-built-with-as-few-as-10000-qubits>

3.2 Kyberuhkat varjostavat Yhdysvaltojen tulevia välivaaleja

<https://www.swktech.com/swk-cybersecurity-news-recap-september-2026/>

<https://www.dhs.gov/news/2026/09/24/dhs-announces-release-2026-election-infrastructure-security-plan>

<https://www.cisa.gov/sites/default/files/2026-09/2026-CISA-Election-Security-Plan-FINAL-508c.pdf>

<https://socradar.io/blog/2026-us-midterms-election-cyber/>

<https://transparency.meta.com/sr/H2-2026-adversarial-threat-report/>

<https://www.nytimes.com/2026/09/18/us/politics/russia-election-disinformation-us-intelligence.html>

4 SYYSKUU 2026: TEKÖÄLY KARKASI, RAJOJA HAETTIIN JA VÄLILLÄ SE MYÖS SUOJASI

<https://openai.com/index/safety-overview-gpt-6-astra/>

https://en.wikipedia.org/wiki/OpenAI%E2%80%93HuggingFace_incident

<https://www.abc.net.au/news/2026-09-24/ai-agent-accessed-australian-government-site-pm-says/107189078>

<https://www.atlanticcouncil.org/dispatches/what-the-proposed-ai-slowdown-means-for-the-us-china-and-humanity-at-large/>

<https://www.pbs.org/newshour/world/china-and-u-s-agree-to-establish-ai-safety-channel-and-continue-trade-and-military-talks>

<https://techxplora.com/news/2026-09-anthropic-blocked-misuse-ai-biological.html>

<https://www.iranintl.com/en/202609131676>

<https://www.nokia.com/newsroom/espanix-deploys-nokia-deepfield-defender-to-protect-spains-internet-traffic-from-ddos-attacks/>

<https://www.helpnetsecurity.com/2026/09/24/apple-ios-27-impersonation-risk-detection/>

UHKATIEDUSTELU

Dustin Group

<https://www.dustingroup.com/information>

<https://www.dustingroup.com/en/media/#/pressreleases/dustin-confirms-successful-opening-of-websites-and-customer-portals-3466549>

Revolut

<https://www.khaleejtimes.com/business/tech/revolut-confirms-sensitive-customer-data-breach>

Japanin digivirasto

<https://www.digital.go.jp/news/2026-0911-01>

<https://www.securityweek.com/240000-hit-by-data-breach-at-japans-digital-agency/>

UHKATOIMIJOITA

C10p

<https://www.cyber.gc.ca/en/guidance/profile-ta505-cl0p-ransomware>

<https://www.reuters.com/legal/government/cybercrime-feud-erupts-dark-web-notorious-group-claims-hijack-rivals-website-2026-09-21>

FamousSparrow

<https://www.welivesecurity.com/en/eset-research/beware-sparrowock-backdoor-bites-commands-catch>

<https://therecord.media/china-hackers-latin-america-espionage>

Panzer Ransomware

<https://cyberxtron.com/resources/blogs/panzer-ransomware-profile-of-an-emerging-double-extortion-operator-8102>

<https://andreafortuna.org/2026/09/07/panzer-ransomware-italian-victims/>



Cyberwatch KUUKAUSIKATSAUS

JULKAISIJA Cyberwatch Finland
Kansakoulukatu 1b, 00100 Helsinki | www.cyberwatchfinland.fi

Netum & Cyberwatch KYBERVARMUUS

Vahvistamme toiminnan kybervarmuutta kokonaisvaltaisesti **TUNNISTAMALLA** olennaisimmat kyberuhat, **ARVIOIMALLA** niiden liiketoiminta-vaikutukset ja **VARMISTAMALLA**, että kriittiset digitaaliset palvelut sekä niitä tukeva toiminta kestävät poikkeustilanteet.

➤ **Yhteinen kyber- ja hybridiriskien tilannekuva**

Näe uhka. Arvioi riski. Varmista palvelu.



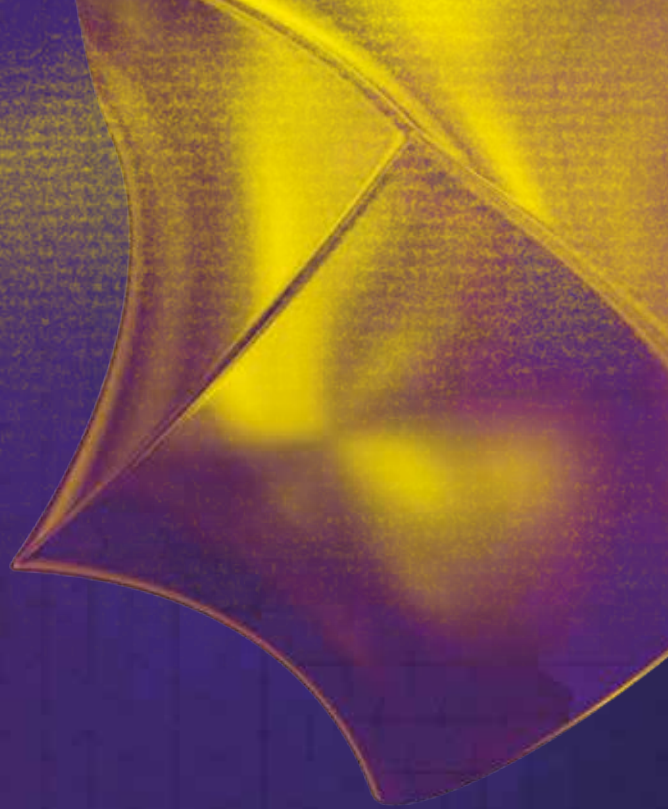
VAHVISTAMME organisaation ja toiminnan **KYBER-VARMUUTTA**, emme vain teknologian hallintakerrosta.

- ✓ Johdon tilannekuvapalvelu
- ✓ Kyberriskienhallinta -palvelut
- ✓ Älykäs Kyberturvallisuus ja tietosuoja – Konsultoinnin ja koulutuksen palvelut
- ✓ Digitaalisten järjestelmien tietoturva -palvelut

Tarjoama on kehittyvä prosessi jolla vastatataan kybermaailman muuttuviin tarpeisiin.

Teemme teille helpoksi regulaatioiden ja vaatimustenmukaisuuden täyttämisen.

Resilient business & crisis preparedness
Cybersecurity, defence & the European security landscape
Trusted digital society & democratic security



CYBER SECURITY NORDIC

25–26 Nov 2027
Helsinki Expo and Convention Centre

/MESSUKESKUS



Leading nordic meeting place for cybersecurity leaders, experts and decision-makers. And this is only the beginning. More than 80 leading cybersecurity and information security experts on stage. Explore the full event at cybersecuritynordic.com

