



Cyberwatch Finland

MAGAZINE 2/2026

Kyberturvallisuus
murroksessa

Cybersecurity
is updating



Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

Tavoitteena kyberkyvykkäämpi maailma



SISÄLTÖ



Pääkirjoitus

> AAPO CEDERBERG



Digitaalinen immuuni-
järjestelmä: Luottamus
syntyy päivittäin,
ei yhdellä päätöksellä

> REPE HARMANEN



Kyberturvallisuus irti
IT-siilosta – Cyber
Security Nordic kokoaa
päättäjät ja asiantuntijat

> ANU EVELIINA MATTILA



Valmiuspohjainen lähestymis-
tapa kyberturvallisuuden
vajeiden tunnistamiseen ja
korjaamiseen kriittisessä
infrastruktuurissa

> EETU LAAKSO, VESA KUIKKA
& KIMMO K. KASKI



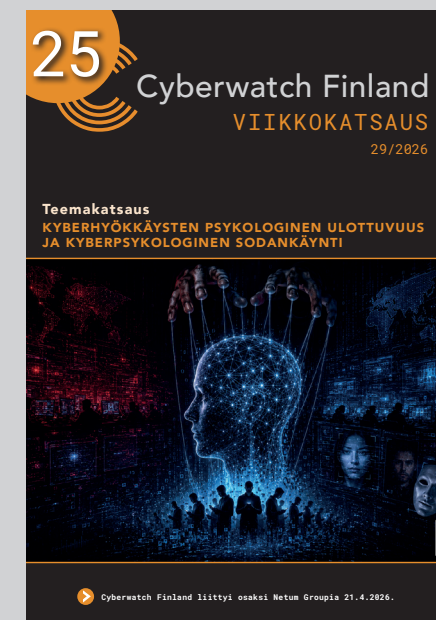
Kaksi ilmiötä,
jotka muuttavat kaiken
turvallisuuteen liittyvän

> KIMMO ROUSKU



Toimintavarmuuden ja
luotettavuuden merkitys
korostuvat entisestään
kyberturvallisuuden muutos-
trendien voimistuessa

> RISTO RAJALA
& PETER SUND



25 Cyberwatch Finland
VIIKKOKATSAUS
29/2026

Teemakatsaus
KYBERHYÖKKÄYSTEN PSYKOLOGINEN ULOTTUVUUS
JA KYBERPSYKOLOGINEN SODANKÄYNTI



Palvelut

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)

Globaali turvallisuusympäristö muuttuu entistä nopeammin. Suurvaltojen ylivoimaa haastavat pienemät valtiot ja yhteenliittymät. Pelkästään sotilaallisella voimalla ei voi voittaa sotia tai erikoisoperaatioita. Elävänä esimerkkinä ovat Lähi-idän konfliktit ja Ukrainan sota. Epäsymmetrisillä keinoilla ja uusilla teknologioilla sekä operatiivisilla toimilla on pystytty haastamaan perinteinen sotilaallisen voiman käyttö ja ylivoima, vaikka sillä on edelleen sunnaton tuhovoima ja kyky tuottaa inhimillisiä tappioita. Konfliktit pitkittyvät ja aiheuttavat entistä suurempia tappioita ja taloudellisia menetyksiä niin konfliktin osapuolille kuin sivullisillekin. Erilaiset keskinäisriippuvuudet tuottavat ikäviä yllätyksiä, kuten Hormuzin salmen

sulkeminen osoitti. Ongelmia aiheutui koko globaalille talousjärjestelmälle. Tulevaisuus näyttää entistä epävarmemmalta ja paikallisten konfliktien määrä näyttäisi kasvavan. Niiden muodot, sisältö sekä vaikutukset tulevat aiheuttamaan yllätyksiä jatkossakin.

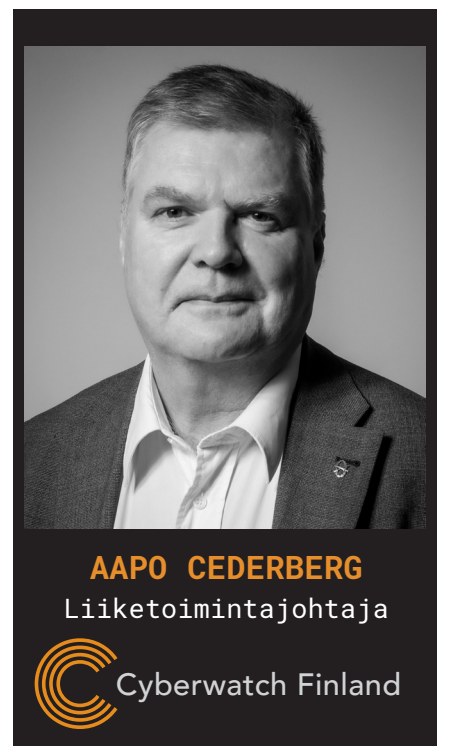
Epävakaassa maailmassa meidän tulee olla entistä vahvempia ja valita tarkemmin liittolaisemme ja kumppanimme. Tämä historiallinen tosiasia ei näyttäisi muuttuvan, ovat kysymyksessä sitten valtiolliset suhteet tai liike-elämän logiikka. Näin mekin olemme ajatelleet Cyberwatchissa. Olemme liian pieni toimimaan yksin, joten menestys edellyttää parempia taloudellisia resursseja ja lisää osaavaa työvoimaa. Tekoälyn käyttöönotto ei yksin riitä, vaan tur-

vallinen ja älykäs ”tekoälyistäminen” vaatii murrosvaiheessa lisäresursseja. Uudistumisnopeus ja innovaatiokyky nousevat arvoon arvaamattomaan. Tätä kaikkea saamme liittymällä osaksi Netum Groupia. Synergiaedut ovat ilmeiset ja Cyberwatchin älykkäät kyberturvallisuuspalvelut ovat tukeva pohja rakentaa Netumille uusi voittava kyberturvallisuuskonsepti. Talo on täynnä osaavia asiantuntijoita ja panostukset tekoälyn hallittuun hyödyntämiseen ovat osa yhteistä strategiaamme. Otamme mielellämme käyttöömme Netumin sloganin ”viisaasti tehty” – se sopii hyvin meidänkin ajatteluunme ja toimintatapaamme.

Kybermaailman murroksesta puhutaan paljon, mutta globaali

epävarmuus ei tee muutoksen vetureiden tunnistamisesta helppoa. Kaikki ymmärtävät, että tekoäly ja kvanttiteknologiat ovat osa murrosta, mutta niiden vaikutuksista ja soveltamismahdollisuuksista onkin jo monenlaisia näkemyksiä. Vain muutos ja sen nopeus näyttäisi olevan varmaa. Kilpailukykyisen hyvinvointiyhteiskunnan kulmakivenä tulevat säilymään digitalisaatio ja siihen liittyvät teknologiat. Turbulentissa maailmassa digitalisaation hyötyjen kotiuttaminen edellyttää suurempia panoksia turvallisuuteen ja erityisesti kyberturvallisuuteen. Siksi älykkäiden ja kustannustehokkaiden kyberturvallisuuspalveluiden sekä teknologioiden merkitys tulee entisestään korostumaan.

EU:n tuottama regulaatio ei yksin takaa parempia kyberturvallisuuspalveluita, mutta se on hyvä heräte kaikille yhteiskunnan kriittisille toimijoille asian tärkeydestä. Olemme tehneet monia asioita oikein, eivätkä tietyt kybermaailman lainalaisuudet ole muuttumassa. Voittava konsepti rakentuu jatkossakin ihmisten osaamisesta, älykkäistä teknologioista ja turvallisista toimintatavoista. Tämä konsepti on hyvä pohja Netumin kyberturvallisuuspalveluiden kehittämiseksi ja juuri se, mihin haluamme panostaa ja tehdä sen viisaasti. Kun uhkakuvat ja riskitekijät muuttuvat, on kyberturvallisuuden oltava entistä ketterämpää ja älykkäämpää. Tässä turvallisuuskulttuurin muutoksessa on pysyttävä perässä ja mieluummin oltava edelläkävijä.





REPE HARMANEN,
NETUM GROUP OYJ

DIGITAALINEN IMMUUNIJÄRJESTELMÄ: Luottamus syntyy päivittäin, ei yhdellä päätöksellä

Kyberturvallisuus ei ole enää yksittäinen tekninen suojaus-toimi eikä määräajoin tarkas-tettava compliance-hanke. Se on organisaation kyky säilyttää toimintakykynsä, todistaa resi-lienssinsä ja ansaita asiakkaiden luottamus joka päivä uudel-leen. Digitaalisessa yhteiskun-nassa luottamus ei synny siitä, ettei mikään koskaan rikkoudu. Se syntyy siitä, että kriittinen palvelu jatkuu myös silloin, kun jokin rikkoutuu.

Uhkataso on kohonnut pysyvästi

Suomen kyberturvallisuuden tilan-kekuva on vakava eikä helpotu. Tra-ficom in Kyberturvallisuuskeskuk-sen vuoden 2025 katsaus kertoo, että vakavien tapausten määrä on pysynyt kahden vuoden ajan ennä-tyksellisen korkealla. Vuosi 2026 on selkeä murrosvaihe: tekoäly vahvis-taa sekä hyökkääjien että puolusta-jien kyvykkyyksiä, ja toimintaym-päristöstä tulee aiempaa nopeampi,

laajempi ja vaikeammin ennakoit-tava.¹

Deepfake-puhelut kuulostavat jo esihenkilöltä. Kalasteluviestit kir-joitetaan virheettömällä suomella. Rikollisuus toimii palveluna ja Ransomware-as-a-Service on arki-päiväistynyt. Tuhoavien haittaohjel-mien määrä kasvaa tasaisesti.²

Perinteinen tapa ajatella kyber-turvallisuutta, jossa rakennetaan muuri, ostetaan lisenssi ja tehdään auditointi kolmen vuoden välein, ei yksinkertaisesti enää riitä. Uhka-

kenttä ei noudata aikataulumme. Se mukautuu jatkuvasti ja meidän on mukauduttava sen mukana.

Haluan tässä artikkelissa esitellä vaihtoehtoisen kehyksen. Organi-saation kyberturvallisuus toimii parhaiten biologisen immuunijär-jestelmän tavoin: se tunnistaa altis-tumisen, reagoi uhkiin ja muistaa jokaisen kohtaamisensa. Sen tehtävä ei ole estää kaikkia hyökkäyksiä, se on mahdotonta. Sen tehtävä on var-mistaa, että selviämme niistä ja jat-kamme toimintaa vahvempina.

**Laki ei enää kysy:
onko suojattu?
Se kysyy: voitko
todistaa resilienssin?**

Vuosi 2026 on eurooppalaisen kyber-lainsäädännön täytäntöönpanossa ratkaiseva. NIS2-direktiivi⁶ on täysi-määräisesti voimassa ja DORA-ase-tusta⁵ on sovellettu finanssisektorilla tammikuusta 2025. Muutos on todel-linen: kyberturvallisuus on juridisoi-tunut.

Asetelma muistuttaa GDPR:n tuloa. Silloinkin moni ajatteli pär-jäävänsä reagoimalla, mutta ei pär-jännyt. Nyt yritysten on pystyttävä osoittamaan resilienssikykyänsä millä hetkellä tahansa, kovan sanktiou-han alla. Kyberturvassa siirrytään lupauksista näyttöihin.³

”Compliance with DORA and NIS2 is not merely a regulatory obligation but a strategic opportunity to build and sustain digital trust.”

– ISACA, 2025⁴

NIS2 koskee laajaa joukkoa toi-mijoita energiasta terveydenhuol-toon ja liikenteestä julkishallintoon. Sanktiot voivat ylittää 10 miljoonaan euroon tai kahteen prosenttiin vuo-tuisesta globaalista liikevaihdosta. Ja vastuu on johdolla. Ei IT-osastolla.⁶

Samaan aikaan valmiuslain uudistamiskeskustelu on nostanut käytäntöön kolme vaatimusta: kriit-tisten toimintojen ylläpitäjien on

kyettävä suunnittelemaan, harjoit-telemaan ja resursoimaan poikkeus-tilanteita varten. Ei kertaluonteisina projekteina, vaan jatkuvana syklinä. Tämä on täsmälleen sama logiikka, jota NIS2 ja DORA kyberturvalli-suudelta edellyttävät. Digitaalinen immuunijärjestelmä ei synny ilman harjoittelua.

**Immuunijärjestelmä
tunnistaa: altistuminen
on kaikkialla**

Törmäämme toistuvasti samaan virheeseen: tietosuoja, kyberturval-lisuus ja IT-palveluiden jatkuvuus hankitaan erillisinä projekteina. Ne eivät ole erillisiä. Ne ovat saman immuunijärjestelmän kerroksia, ja järjestelmä on vain niin vahva kuin sen heikoin kerros. Heikoin lenkki ei välttämättä ole oma järjestelmä, vaan alihankkija, integraatorajapinta tai kumppanin tietoturvaso.

**Kerros 1: Tietosuoja
– henkilötietojen
suojaus on perusoikeus**

GDPR-velvoitteet ovat tuttuja, mutta niiden tosiasiallinen noudattaminen on vuosi vuodelta monimutkaisem-paa. Tekoälyn yleistymisen lisää pai-netta entisestään: tekoälypohjaisten järjestelmien tietosuoja- ja tietotur-vavaatimukset edellyttävät tarkkaa sisäistä ohjeistusta.⁹ Meillä Netu-milla julkisen sektorin asiakkaat muistuttavat siitä päivittäin. Kun ajanvaraus, potilastieto, lupakäsit-tely tai kansalaispalvelu pysähtyy, kyse ei ole teknisestä häiriöstä. Kyse on luottamuksen häiriöstä.

**Kerros 2: Kyber-
turvallisuus – näkyvä
ja näkymätön uhkapinta**

Kyberhyökkäykset eivät kohdistu enää vain suoraan yrityksiin. Ne iskevät sinne, missä suoja on hei-kointa: toimitusketjuihin, alihank-

kijoihin, integraatioihin. Organi-saation digitaalinen immuunijärjes-telmä ei pääty omaan palomuriin. Se ulottuu toimitusketjuun, alihank-kijoihin, integraatioihin ja kumppa-neiden toimintakykyyn.¹⁰

Cyberwatch Finlandin kehittämä darkSOC-analyysi tarjoaa näkymän organisaation altistumistasoon myös pimeässä ja syvässä verkossa. Dataa kerätään jatkuvasti hakkerifooru-meilta, tietomurtojen jakoalustoilta ja pimeän verkon markkinapaikoilta, jopa 9 gigatavua sekunnissa, ympäri vuorokauden.⁸ Näin muodostuu kuva siitä, miltä organisaatio näyt-tää vihamielisen toimijan silmin. Tieto siitä, mistä olet altistunut, on hyvin erilainen lähtökohta kuin yllä-tys hyökkäyksen jälkeen.

**Kerros 3: IT-palvelun
jatkuvuus – toiminta
ei saa pysähtyä**

Tätä kerrosta aliarvioidaan eniten. Kriittinen infrastruktuuri, julki-nen sektori ja terveydenhuolto ovat yhteiskunnan selkäranka, eikä nii-den palveluiden katkeaminen ole tekninen häiriö, vaan vakava asia.⁷ DORA edellyttää jatkuvaa ICT-jär-jestelmien monitorointia, anoma-lioiden havaitsemismekanismeja sekä testattua palautumiskykyä.¹⁰ 24/7-valvonta, ennakoiivat päivityk-set ja harjoiteltu jatkuvuussuunni-telma eivät ole luksustavaraa. Ne ovat hintansa arvoisia juuri silloin, kun kaikki muu menee pieleen. Digitaali-nen immuunijärjestelmä reagoi näin.

**Netum+Cyberwatch
Finland: Kyberturva
osaksi luottamuksen
johtamista**

Cyberwatch Finlandin liittyminen Netumiin ei ollut sattumaa.⁹ Meille kyberturvallisuus ja tietosuoja eivät ole päälle liimattuja lisäosia, vaan ne ovat strateginen läpileikkaava vahvuus. Tämä korostuu erityisesti kasvaessamme data-, integraatio- ja

tekoälyratkaisuihin sekä laajentuesamme yksityiselle sektorille.

Cyberwatch Finland tuo Netumiin kyvyn katsoa kyberturvaa johdon, sääntelyn, riskin, toimitusketjun ja jatkuvuuden näkökulmista.⁸ Tämä täydentää Netumin teknistä toteutuskykyä: emme ainoastaan rakenna järjestelmiä, vaan autamme asiakkaita varmistamaan, että ne kestävät painetta. Palvelumme ulottuvat tilannekuva- palvelusta ja darkSOC-analysistä aina yritysjärjestelyjen Cyber Due Diligence -arviointeihin.

Aapo Cederberg, Cyberwatch Finlandin perustaja, kiteyttää asian hyvin:

”Kestävä kyberturvallisuus lähtee ylimmältä johdolta – sieltä, jossa kyberriskien hallinta on olennainen osa hyvää hallintoa ja yritys vastuuta.”

Tähän on helppo yhtyä. Sijoittajat, asiakkaat ja viranomaiset eivät jatkossa kysy vain mitä organisaatio sanoo suojaavansa. Ne kysyvät mitä se pystyy osoittamaan, testaamaan ja todentamaan. Minimivaatimusten täyttäminen ei riitä.

Immuunijärjestelmä muistaa ja vahvistuu: ISO 27001 ja yritys- turvallisuusselvitystodistus

ISO 27001 ei ole meille seinälle kehystetty todistus, vaan digitaalisen immuunijärjestelmämme perusrakenne. Se kattaa koko konsernin ratkaisuliiketoiminnot.⁹ Se tarkoittaa dokumentoitua, auditoitua ja jatkuvasti kehittyvää tapaa johtaa tietoturvaa, ei yksittäistä sertifikaattia hyllyssä. Sertifiointia on ylläpidetty

katkeamattomasti jo yli kahden vuosikymmenen ajan.

Yritysturvallisuusselvitystodistus puolestaan osoittaa, että täytämme viranomaisten vaatimukset turvallisuusluokiteltujen tietojen käsittelylle. Julkisen sektorin hankinnoissa se on konkreettinen näyttö siitä, että tietojen luottamuksellisuus, eheys ja saatavuus on hoidettu kunnolla. Ei lupaus, vaan osoitettu tosiasia.

Tietoturva ei Netumilla ole vain IT-tiimin asia. Koko henkilöstö koulutuu vuosittain ja toimintamallit tietoturvapoikkeamien raportointiin ovat selkeät. Se on kulttuuri.⁹

CWF:n osaaminen johdon koulutuksessa, skenaarioharjoittelussa ja riskienhallinnassa vahvistaa tätä kulttuuria entisestään. Digitaalinen immuunijärjestelmä vahvistuu, kun koko organisaatio harjoittelee, oppii ja muistaa.

Digitaalinen immuunijärjestelmä ja käytännön johtopäätökset

Biologinen immuunijärjestelmä ei ole muuri. Se tunnistaa altistumisen, reagoi uhkiin, palautuu häiriöistä ja vahvistuu jokaisesta kohtaamisesta. Juuri tätä organisaatioilta nyt vaaditaan.

Digitaalinen immuunijärjestelmä ei ole yksittäinen teknologia, standardi tai palvelu. Se on tapa johtaa luottamusta. Organisaatio, jolla se on, kykenee:

- tunnistamaan altistumistonsa myös näkymättömässä verkossa,
- reagoimaan uhkiin ennen kuin ne realisoituvat häiriöiksi,
- jatkamaan palvelutuotantoaan häiriötilanteessa,
- osoittamaan resilienssikykyänsä viranomaisille, asiakkaille ja sijoittajille.

Nämä ovat johtamistapoja. Ja ne ovat kilpailuetuja myös siksi, että ne rakennetaan ennen kuin niitä tarvitaan.

Siksi vastuullisen organisaation kysymys ei ole enää lain minimivaatimusten täyttäminen. Kysymys on, pystyykö se katsomaan asiakasta, viranomaista ja sijoittajaa silmiin ja osoittamaan: olemme varautuneet, olemme harjoitelleet ja palvelumme kestää.⁸

Me Netumilla vastaamme tähän omalla toiminnallamme. ISO 27001-pohjainen hallintajärjestelmä, yritysturvallisuusselvitystodistus ja Cyberwatch Finlandin strateginen kyberturvallisuusosaaminen muodostavat yhdessä digitaalisen immuunijärjestelmän, joka tunnistaa, reagoi ja vahvistuu. Luottamus ei synny siitä, ettei mikään koskaan rikkoudu. Se syntyy siitä, että palvelu kestää, palautuu ja vahvistuu.

LÄHTEET

- 1 Traficom / Kyberturvallisuuskeskus: ”Kyberturvallisuuden vuosi 2025 – uhkataso pysyi kohonneena, vakavien tapausten määrät kasvavat”. Julkaistu 29.1.2026. <https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuden-vuosi-2025-uhkataso-pysyi-kohonneena-vakavien-tapausten-maarat>
- 2 Elisa Yrityksille: ”Kyberturvallisuus 2026: yhdeksän havaintoa Suomesta”. Julkaistu 29.10.2025. <https://yrityksille.elisa.fi/ideat/kyberturvallisuuden-trendit-vuonna-2026-ai-vastaan-ai-ja-8-muuta-havaintoa/>
- 3 DPO Consulting: ”ISO 27001, NIS2 and DORA: Building Sustainable Cyber Compliance in 2026”. Julkaistu 4.2.2026. <https://www.dpo-consulting.com/blog/iso-27001-nis2-and-dora-building-sustainable-cyber-compliance-in-2026>
- 4 ISACA: ”DORA and NIS2: Connection Points and Key Differences”. Julkaistu 5.6.2025. <https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2025/dora-and-nis2-connection-points-and-key-differences>
- 5 Euroopan parlamentin ja neuvoston asetus (EU) 2022/2554 digitaalisen operatiivisen häiriönsietokyvyn vaatimuksista rahoitussektorille (DORA). Sovellettavissa 17.1.2025 alkaen.
- 6 Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 verkko- ja tietojärjestelmien turvallisuudesta (NIS2). Voimaansaattettu kansalliseen lainsäädäntöön 2024–2025.
- 7 NetNordic: ”Pilvipalvelujen turvallisuus vuonna 2026: hallinta, vaatimustenmukaisuus ja jatkuvuus”. Julkaistu 25.2.2026. <https://netnordic.fi/insights/pilvipalvelujen-turvallisuus-vuonna-2026/>
- 8 Cyberwatch Finland: Yritysesittely ja palvelukuvaukset 2025. <https://www.cyberwatchfinland.fi>
- 9 Netum Group Oy: Vuosikertomus 2025. Julkaistu maaliskuussa 2026. <https://netum.fi/sijoittajille>
- 10 ISACA: ”Resilience and Security in Critical Sectors: Navigating NIS2 and DORA Requirements”. White paper 2025. <https://www.isaca.org/resources/white-papers/2025/resilience-and-security-in-critical-sectors-navigating-nis2-and-dora-requirements>



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. Keväällä 2026 Netumiin liittyi Cyberwatch Finland, vuonna 2017 perustettu strategisen kyberturvallisuuden asiantuntijatalo. Tämä artikkeli syntyi juuri siitä yhdistymisestä innostuneena.

REPE HARMANEN
Toimitusjohtaja
Netum Group Oyj



ANU EVELIINA MATTILA,
CYBER SECURITY NORDIC

Messukeskus Mediabank

Kyberturvallisuus irti IT-siilosta – CYBER SECURITY NORDIC KOKOAA PÄÄTTÄJÄT JA ASiantuntijat

Kyberturvallisuus ei ole enää yksittäinen funktio organisaatiossa, vaan keskeinen osa liiketoiminnan jatkuvuutta, luottamusta ja yhteiskunnan vakautta. Cyber Security Nordic on vakiinnuttanut asemansa pohjoismaisen kyberturvakentän foorumina, joka tuo alueelle mielenkiintoisia kansainvälisiä keynote-puheenvuoroja. Tapahtuma järjestetään seuraavan keran Helsingin Messukeskuksessa 28.–29.10.2026.

Euroopan kyberturvallisuustapahtumien kentässä Cyber Security Nordic asettuu kiinnostavasti kahden ääripään väliin. Toisaalla ovat massiiviset, globaalit konferenssit, joissa mittakaava tuo näkyvyyttä mutta usein hajottaa kokonaiskuvaa. Toisaalla taas pienemmät ja rajatut tapahtumat. Cyber Security Nordic edustaa strategisesti ohjattua keskikokoa: tapahtumaa, jossa laajuus ja syvyys pysyvät tasapainossa.

”Kyberturvallisuus on liikkunut pois IT-siilosta suoraan liiketoimintajohdon agendalle. Cyber Security Nordicissa rakennamme kokonaiskuvaa, jossa teknologia, riskit ja markkina kohtaavat ilman hypeä, ja tiukasti kiinni toimintaympäristön todellisuudessa”, sanoo tapahtuman Cyber Security Nordicin tuottaja Miina Miettinen.

Toimialan ammattilaisten suunnittelema ohjelma, joka rakentaa ymmärrystä

Vuosittain järjestettävä kaksipäiväinen tapahtuma on kasvanut kokonaisuudeksi, jossa sisältö, verkostoituminen ja näkökulmat rakentuvat harkituksi ekosysteemiksi. Tänä syksynä tapahtuma laajenee isompiin tiloihin ja kokoaa jälleen yhteen asiantuntijat, johtajat, kriittisen infrastruktuurin päättäjät sekä kyberturvallisuusratkaisujen tarjoajat.

Keskeinen erottava tekijä on ohjelman suunnittelu. Sisältö rakentuu valittujen teemojen ja kohderyhmän tarpeiden ympärille, ja kansainväliset sekä kotimaiset asiantuntijat tuovat keskusteluun useita näkökulmia. Puheenvuorot eivät jää irrallisiksi, vaan muodostavat kokonaisuuden, joka auttaa ymmärtämään kyberturvallisuuden kehityssuuntia ja vaikutuksia käytännössä.

Tunnelmassa korostuu luottamus, laatu ja pohjoismainen avoimuus

Cyber Security Nordicia ohjaa vahvasti pohjoismainen toimintakulttuuri, joka näkyy kolmessa keskeisessä periaatteessa.

Luottamus. Pohjoismaissa kyberturvallisuuden vahvuus syntyy toimijoiden välisestä luottamuksesta, avoimesta tiedonjaosta ja yhteisestä tilannekuvasta. Cyber Security Nordic vahvistaa tätä kulttuuria tarjo-

amalla asiantuntevaa ja läpinäkyvää keskustelua.

On mistä valita. Ohjelma keskittyy olennaiseen. Teemat heijastavat ajankohtaisia ilmiöitä, kuten geopoliittista tilannetta, tekoälyn murrosta, sääntelyn vaikutuksia ja kriisinkestävyyttä, ja ulottuvat strategiasta aina käytännön toteutukseen asti.

Avoin ilmapiiri. Osallistujat eivät ole vain yleisöä, vaan osa keskustelua. Ihmisen kokoinen tapahtuma mahdollistaa sekä huippupuheenvuorojen seuraamisen että aidot kohtaamiset.

Kolme tasoa ymmärrystä – yksi kokonaisuus

Cyber Security Nordic rakentuu kolmen ohjelman ja Traficom Tietoturvaseminaarin ympärille.

Stage One keskittyy strategiseen tasoon: kyberturvallisuuteen geopoliittisena voimana, johtamisen kysymyksenä ja liiketoimintariskinä. Ohjelma rakentuu kansainvälisistä keynote-puheenvuoroista ja johtajien näkemyksistä, joita harva on kuullut aikaisemmin.

Gold Stage ja Scandium Stage tuovat keskustelun lähemmäs käytäntöä käsittelemällä esimerkiksi IT/OT-ympäristöjä, pilviriippuvuutta ja hyökkääjien toimintamalleja. Scandium Stagella on tapahtuman toisena päivän Traficom Tietoturvaseminaari, joka tarjoaa katsauksen ajankohtaisiin kyberturvallisuuden uhkisiin, viranomaisen toimiin ja digitaalisen yhteiskunnan turvallisuuteen.

Hacker's Corner tuo ohjelmaan käytännönläheisen, hands-on-ulottuvuuden: lyhyitä demoja, työpaikkoja ja live-case-analyyskejä, joissa osallistujat pääsevät syventymään esimerkiksi phishingin purkuun, OSINT-tiedonhakuun, uhkamallinukseen ja SOC-simulaatioihin sekä eettisiin näkökulmiin.

Yhdessä nämä muodostavat kokonaisuuden, joka palvelee yhtä aikaa johtoa, asiantuntijoita ja operatiivisia toimijoita.

Kohtaamiset ovat osa kokonaisuutta

Tapahtuman keskeinen arvo syntyy myös kohtaamisista. Laaja näytelyalue tuo yhteen kyberturvallisuusyritykset, asiantuntijat ja organisaatiot, jolloin keskustelut lavalla jatkuvat käytännön tasolle.

Tämä mahdollistaa markkinan ymmärtämisen laajemmin: teknologiat, ratkaisut ja kokemukset asettuvat samaan yhteyteen. Verkostoituminen ei ole sivuroolissa, vaan olennainen osa kokonaisuutta.

Ajankohtaiset teemat vuodelle 2026

Vuoden 2026 ohjelmassa korostuvat kolme teemakokonaisuutta:

- **Resilient business & crisis preparedness**, jossa tarkastellaan liiketoiminnan jatkuvuutta, toimitusketjujen riskejä sekä NIS2- ja DORA-vaatimuksia
- **Cybersecurity, defence & the European security landscape**, jossa keskiössä ovat geopoliittiset riskit ja hybridihaikuttaminen
- **Trusted digital society & democratic security**, jossa tarkastellaan disinformaatiota, tekoälyn vaikutusta ja luottamusta digiyhteiskunnassa

Yhteisenä nimittäjänä on kyberturvallisuuden rooli laajasti yhteiskunnallisena ja taloudellisena ilmiönä.

Kulissien takana

Tapahtuman ohjelma syntyy pitkäjänteisen työn tuloksena. Suunnittelu alkaa pian edellisen tapahtuman jälkeen määrittelemällä keskeiset teemat ja ilmiöt.

Tämän pohjalta rakennetaan puhujaprofiilit ja sisältökokonaisuus,

jossa yhdistyvät kansainvälinen näkökulma, pohjoismainen konteksti ja käytännön kokemus. Lähtökohtana on osallistujan näkökulma: mitä uutta tietoa, ymmärrystä tai kontakteja hän saa mukaansa.

Missä Cyber Security Nordic erottuu

Cyber Security Nordicin asema Euroopassa rakentuu kolmen tekijän varaan: mittakaava, kuratointi ja keskustelukulttuuri.

Se on riittävän suuri tuodakseen yhteen alan keskeiset toimijat, mutta riittävän fokuoitu säilyttää keskustelun laadun. Ohjelman kuratointi varmistaa, että sisältö rakentaa kokonaiskuvaa, ja pohjoismainen avoimuus luo tilaa suoralle ja analyttiselle keskustelulle.

Tapahtumassa on myös näyttävyyttä, mutta se tukee sisältöä – ei korvaa sitä.

Yhdessä nämä luovat tapahtumalle aseman, jossa fokus ei ole pelkästään näkyvyydessä, vaan siinä, että osallistuja lähtee kotiin aidosti viisaampana ja paremmin verkostoituneena.

KIRJOITTAJA:



ANU EVELIINA MATTILA
Marketing and Communications,
Cyber Security Nordic,
Helsinki Expo and Convention Centre
(Messukeskus)



> EETU LAAKSO,
VESA KUIKKA &
KIMMO K. KASKI

Valmiuspohjainen lähestymistapa kyberturvallisuuden vajeiden tunnistamiseen ja korjaamiseen kriittisessä infrastruktuurissa

Kyberuhkien määrä on kasvanut nopeasti kaikkialla maailmassa, ja terveydenhuolto on toistuvasti yksi useimmin kohteeksi joutuvista kriittisen infrastruktuurin sektoreista¹, osin siksi, että sen ydintehtävä on potilaiden hoito eikä kyberturvallisuus, ja osin siksi, että arkaluontaisen potilastiedon on oltava jatkuvasti saatavilla. Kyberturvallisuuden parhaista käytännöistä on tarjolla runsaasti laadukasta ohjausta, kuten ISO 27000 -sarja ja NIST Cybersecurity Framework 2.0². Nämä viitekehykset kertovat, mitä organisaation kannattaisi tehdä, mutta tarjoavat rajallisesti ohjausta siihen, missä järjestyksessä ja millä painotuksella toimenpiteet kannattaa toteuttaa. Tämä on erityisen tärkeä näkökulma pienissä ja keskisuurissa yrityksissä, joissa resurssit ovat niukat³.

Tässä artikkelissa esittelemme, miten alun perin puolustussektorille

kehitettyä valmiuspohjaista arviointimallia⁴ voidaan soveltaa kyberturvallisuuden päätöksenteon tueksi. Testasimme mallia yksityisessä terveydenhuolto-organisaatiossa, jolla ei ole omaa IT- tai kyberturvallisuusyksikköä, mutta joka kuuluu NIS2-direktiivistä johdetun kansallisen kyberturvallisuuslainsäädännön piiriin.

Menetelmä pähkinänkuoressa

Mallissa kyberturvallisuusvalmius jaetaan osavalmiuksiin, kuten esimerkiksi hallintoon, pääsynhallintaan, valvontaan ja kriisiviestintään. Kullekin osavalmiukselle määritellään tavoitetaso: mitä organisaatiolta voidaan kohtuudella odottaa sen koon, toimialan ja käytettävissä olevien resurssien perusteella. Nyky-

tilan ja tavoitetason välinen ero on *valmiusvaje*. Mitä suurempi vaje, sitä kauempana organisaatio on tavoitetasostaan.

Kaikki vajeet eivät kuitenkaan ole yhtä vakavia. Siksi jokaiselle osavalmiukselle annetaan myös tärkeys-paino, joka kuvaa, kuinka vakavat seuraukset olisivat, jos vaje jäisi korjaamatta. Kaksi yhtä suurta vajetta voivat siis painaa lopputuloksessa eri tavalla riippuen siitä, kuinka kriittisestä asiasta on kyse.

Kun organisaatio harkitsee parannustoimenpiteitä, esimerkiksi henkilöstön lisäämistä, henkilöstön koulutusta tai uutta hallintamallia, malli laskee, kuinka paljon kukin toimenpide pienentää kutakin havaittua vajetta suhteessa sen kokonaispanokseen. Tämä tekee näkyväksi, mitkä toimenpiteet tuottavat eniten parannusta suhteessa käytettyyn vaivaan, ja mahdollistaa eri parannuspolku-

jen, kuten esimerkiksi ”suurin vaikutus” vai ”pienin vaiva” vertailun ennen resurssien sitomista.

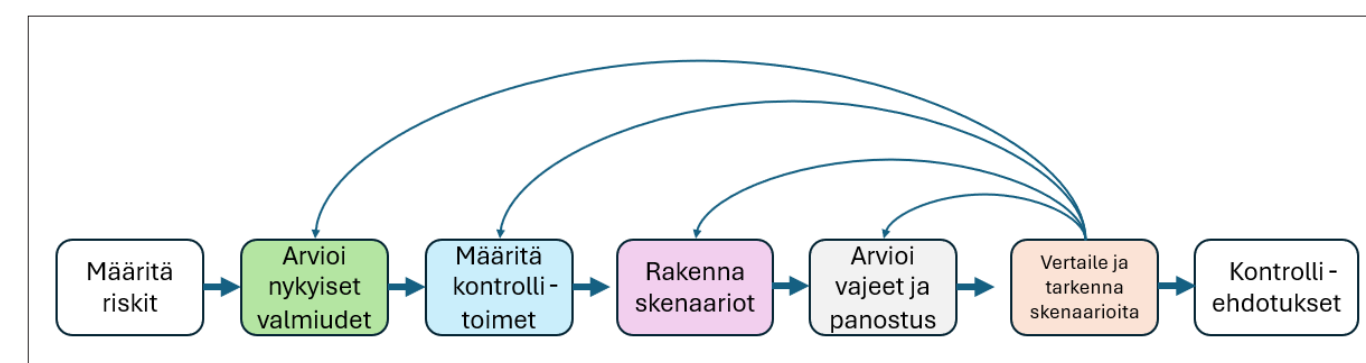
Käyttötapaus: terveydenhuolto-organisaatio

Sovelsimme mallia yksityiseen terveydenhuolto-organisaatioon, joka tuottaa jatkuvia hoivapalveluita

useissa toimipisteissä. Organisaatiolla ei ole omaa IT-osastoa, vaan kyberturvallisuustoiminnot on pitkälti ulkoistettu ja vastuut on jaettu ”monta hattua” -periaatteella. Silti organisaatio kuuluu Suomen kansalliseen kriittiseen infrastruktuuriin, ja sen palveluista on riippuvainen merkittävä määrä ihmisiä.

Mallin syötteenä käytimme organisaation olemassa olevaa IT-riskikirjanpitoa, jossa riskit oli

jo luokiteltu strategisiin, operatiivisiin ja taktisiin riskeihin. Tulkitimme jokaisen riskin merkinä taustalla olevasta valmiusvajeesta ja kartoitimme sen yhteen tai useampaan osavalmiuteen. Kuva 1 havainnollistaa koko työnkulun: riskien tunnistamisesta valmiuksien arviointiin, toimenpiteiden määrittelyyn, skenaarioiden rakentamiseen ja lopulta vertailuun ennen päätöksentekoa.



Kuva 1. Valmiuspohjainen työnkulku kyberturvallisuuden parantamiseksi: riskien määrittelystä skenaarioiden vertailuun ja iteratiiviseen tarkentamiseen ennen kontrollipäätöksiä.

Tulokset: kaksi parannusskenaariota

Rakensimme kaksi vertailevaa parannusskenaariota, joissa kummassakin valittiin kolme toimenpidettä käytettäväksi rajallisella suunnittelujaksolla. Skenaario 1 (”suuri vaikutus”) priorisoi toimenpiteitä, jotka pienentävät eniten tärkeys-painotettuja vajeita: valituiksi tulivat henkilöstön riittävyys, kriisiviestintäohjeistus ja -harjoitukset sekä kyberturvallisuuden hallintamallin luominen. Skenaario 2 (”vähäinen vaiva”) priorisoi toimenpiteitä, joiden arvioitu toteutuspanostus oli pienin.

Skenaario 1 pienensi jäljellä olevaa tärkeyspainotettua valmiusvajetta noin 13 %, kun taas Skenaario 2 saavutti noin 9 %:n vähenemän. Suuren vaikutuksen strategia tuotti siis selvästi suuremman suhteellisen parannuksen, mutta myös vähäi-

sen vaivan strategia toi merkityksellistä hyötyä, mikä on tärkeä havainto organisaatioille, joilla ei ole varaa toteuttaa kaikkein kalleimpia toimenpiteitä kerralla.

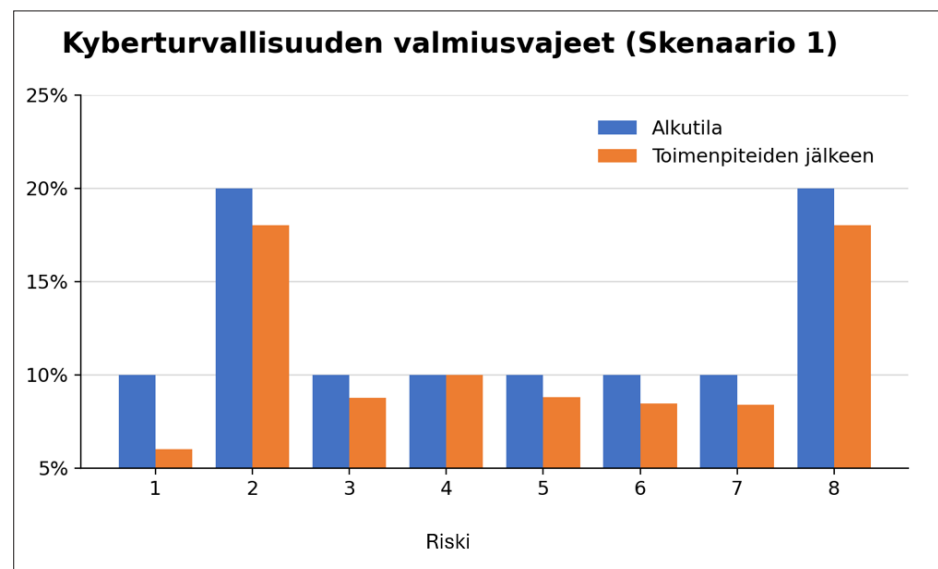
Kuva 2 näyttää, miten vajeet pienenevät eri riskien osalta Skenaariossa 1: vähennys ei ollut tasainen kaikkialla, vaan erityisen suuri parannus näkyi heikkoon kyberturvallisuushallintoon liittyvässä riskissä (Riski 1). Tämä kertoo siitä, että valitut toimenpiteet osuivat erityisen hyvin juuri niihin osavalmiuksiin, jotka olivat kyseisen riskin taustalla.

Johtopäätökset

Tulokset osoittavat, että alun perin sotilaskäyttöön kehitetty valmiuspohjainen malli soveltuu myös kyberturvallisuuden päätöksenteon tueksi resurssirajoitteisessa kriit-

tisessä infrastruktuurissa. Malli ei kerro absoluuttista totuutta organisaation turvallisuustasosta, vaan toimii vertailevana päätöstukena: se auttaa näkemään, mitkä toimenpiteet tuottavat eniten hyötyä suhteessa vaivaan, ja tekee priorisointiperusteet läpinäkyviksi ja sitä kautta helpottaa päätöksentekijää tekemään päätöksen investoinneista.

On syytä huomata, että kyseessä on yksittäinen tapaustutkimus, ja mallin siirrettävyys puolustussektorilta kyberturvallisuuteen on tässä vaiheessa oletus pikemminkin kuin tiukasti todistettu tulos. Myös vajeiden ja toimenpiteiden vaikutusten arviointi perustui yhden asiantuntijan näkemykseen. Jatko-tutkimuksessa aiomme soveltaa mallia useampiin organisaatioihin ja eri kriittisen infrastruktuurin sektoreille sekä ottaa mukaan useampia arvioijia mallin yleistettävyyden ja luotettavuuden parantamiseksi.



Kuva 2. Skenaario 1:n vaikutus kyberturvallisuuden valmiusvajeisiin riskeittäin: alkuperäinen vaje verrattuna vajeeseen toimenpiteiden jälkeen. Riskit: 1) heikko kyberturvallisuushallinto, 2) maineriski, 3) toimitusketjun häiriöt, 4) sääntelyn noudattamatta jättäminen, 5) puutteellinen tiedonhallinta, 6) tekninen valmiuden puute, 7) tietomurto tai sen manipulointi, 8) hyökkäyksen jälkeinen maine- ja sääntelyvaikutus.

LÄHTEET

- 1 ENISA (2023) Health Threat Landscape Report. European Union Agency for Cybersecurity. Saatavilla: <https://www.enisa.europa.eu/publications/health-threat-landscape> (haettu 18.1.2026).
- 2 National Institute of Standards and Technology (2024) Cybersecurity Framework 2.0. NIST, Gaithersburg. Saatavilla: <https://www.nist.gov/cyberframework> (haettu 27.12.2025).
- 3 El-Hajj, M. ja Mirza, Z.A. (2024) "Protecting Small and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool", Electronics, 13(19), artikkeli 3910. doi:10.3390/electronics13193910
- 4 Kuikka, V. ja Peltotalo, S. (2022) "A Method for Assessing Effects of Technological Development on Military Capabilities", Proceedings of the International Conference on Decision Aid Sciences and Applications (DASA), IEEE, s. 1634–1639.

KIRJOITTAJAT:

EETU LAAKSO

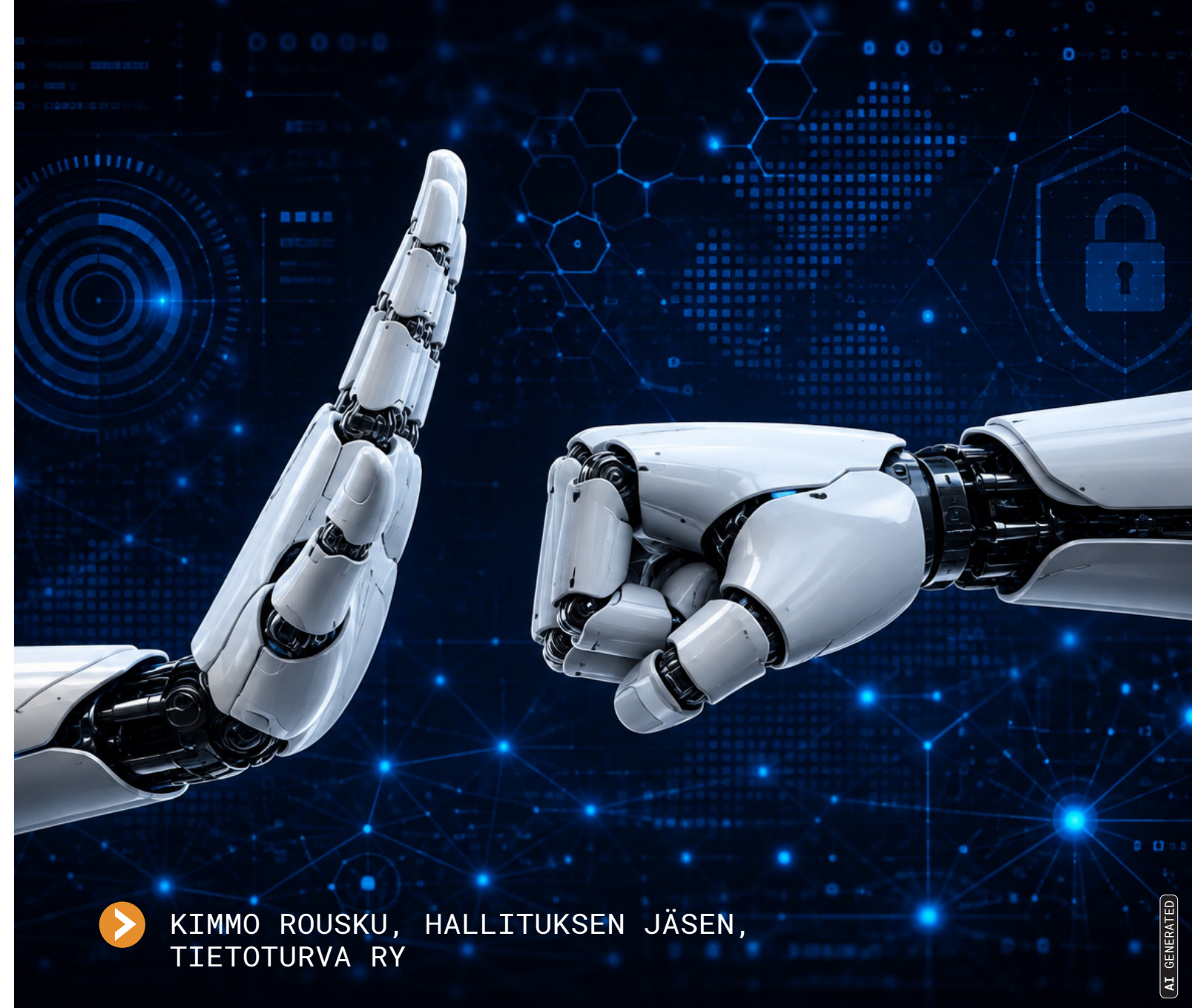
Eetu Laakso työskentelee Cyberwatch Finlandilla (osa Netum Groupia) mm. kyberturvallisuuden hallinnon, riskienhallinnan ja vaatimustenmukaisuuden (GRC) parissa. Hän on suorittanut farmasian kandidaatin tutkinnon Helsingin yliopistossa sekä ICT:n ja kyberturvallisuuden DI (M.Sc.) Turun yliopistossa. Tämä artikkelin tiivistelmä perustuu hänen ensimmäiseen tieteelliseen julkaisuunsa.

VESA KUIKKA

Vesa Kuikka on suorittanut sotatieteiden tohtorin tutkinnon Maanpuolustus-korkeakoulussa (2021) sekä tekniikan tohtorin (D.Sc.) tutkinnon Aalto-yliopistossa (2022). Hänen tutkimuksensa käsittelee sotilaallisten valmiuksien mallintamista, stokastista taistelunkulkua ja verkostokeskeistä sodankäyntiä, kompleksisia verkostoja, kyberanalyysiä, tiedon leviämistä sekä resilienssiä, hyödyntäen tilastollista fysiikkaa, todennäköisyyspohjaista mallinnusta ja systeemitekniikkaa.

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 tietoaisteiden data-analytiikkaa että laskennallisia mallinnusmenetelmiä.



KIMMO ROUSKU, HALLITUKSEN JÄSEN,
TIETOTURVA RY

AI GENERATED

Kaksi ilmiötä, jotka muuttavat kaiken turvallisuuteen liittyvän

Tekoäly muuttaa samanaikaisesti sekä hyökkäämistä että suojautumista. Samaan aikaan tekoäly paljastaa ohjelmistoista sellaisen määrän haavoittuvuuksia, ettei entinen tapa seurata, arvioida ja asentaa tietoturvapäivityksiä enää riitä. Nämä kaksi ilmiötä eivät muuta vain kyberturvallisuutta. Ne muuttavat riskienhallintaa, jatkuvuutta, varautumista, tietoturvaa ja tietosuoja.

Tulos voi olla 112–13

Kuvitellaan koripallo-ottelu, jossa toisella puolella on ihminen ja toisella tekoäly tehokkaasti hyödyn-tävä vastustaja. Lopputulos saattaa olla tyyli: 112–13.

Ihminen ei pysty valvomaan miljoonia tapahtumia samanaikaisesti, tutkimaan valtavia määriä ohjelma-koodia, vertaamaan havaintoja kaikkiin tunnettuihin haavoittuvuuksiin

eikä reagoimaan sekunneissa jokaiseen poikkeamaan. Tekoäly pystyy tekemään tätä tauotta, ympäri vuorokauden ja valtavalla nopeudella – siis ihan oikeasti 24/7.

Mutta ottelu ei ole menetetty!

Kun ihminen ottaa tekoälyn avukseen, voimme päästä tasoihin. Tekoäly tuo nopeuden, mittakaavan ja kyvyn käsitellä valtavia tietomääriä. Ihminen tuo toimintaympäristön ymmärryksen, arvot,

vastuun, harkinnan ja kyvyn tehdä päätöksiä epävarmuuden keskellä. Näiden inhimillisten ominaisuuksien avulla voimme myös voittaa. Siksi oma ohjeeni on yksinkertainen: tekoäly on otettava käyttöön kaikessa suojautumisessa. Ei poistamaan ihmistä turvallisuustyöstä, vaan vahvistamaan ihmisen kykyä nähdä, ymmärtää, ennakoida ja toimia. Jos hyökkääjä käyttää tekoälyä ja puolustaja ei, ottelu ei ole reilu.

Haavoittuvuuksien löytymisen fysiikka muuttui

Tekoälymallien kyky löytää ohjelmistojen haavoittuvuuksia on kasvanut erittäin nopeasti. Anthropic kertoi helmikuussa 2026 löytäneensä ja validoineensa Claude-mallin avulla

yli 500 vakavaa haavoittuvuutta avoimen lähdekoodin ohjelmistoista. Osa haavoittuvuuksista oli säilynyt huomaamatta jopa vuosikymmeniä. Malli ei vain etsinyt tuttuja koodivirheitä, vaan päätteli ohjelman toimintaa, tutki aikaisempia korjauksia ja löysi vastaavia korjaamatta jääneitä kohtia.¹

Microsoft puolestaan ilmoitti ottaneensa käyttöön MDASH-järjestelmän, jossa yli sata erikoistunutta tekoälyagenttia etsii, arvioi, haastaa ja todentaa mahdollisia haavoittuvuuksia. Toukokuun 2026 tietoturvapäivityksiin sisältyi 16 tällä järjestelmällä löydettyä haavoittuvuutta, joista neljä oli kriittisiä etäkoodin suorittamisen mahdollistavia haavoittuvuuksia.²

Microsoft varoitti heinäkuussa suoraan, että asiakkaiden pitää valmistautua aikaisempaa suurempiin päivitysmääriin. Yhtiön mukaan

tekoäly löytää enemmän ongelmia, nopeammin ja laajemmista ohjelmistokokonaisuuksista³. OpenAI on kuvannut muutosta vielä suuremmin: aikaisemmin pullonkaulana oli haavoittuvuuksien löytäminen, mutta nyt pullonkaulaksi on muodostumassa niiden korjaaminen⁴. Tämä on valtava muutos!

Päivitysmäärät kertovat suunnan

Alla olevat luvut eivät ole keskenään täysin vertailukelpoisia. Microsoft julkaisee kuukausittaisia kokonaisuuksia, mutta Oracle käyttää sekä kohdennettuja kuukausipäivityksiä että laajoja neljännesvuosittaisia päivityksiä. Linux ei ole yksi valmistaja vaan laaja ekosysteemi. Taulukko kertoo silti erittäin selvästi, mihin suuntaan olemme menossa.

KOHDE JA LASKENTATAPA	TOUKOKUU 2026	KESÄKUU 2026	HEINÄKUU 2026
Microsoft Patch Tuesday	120 haavoittuvuutta, joista 29 kriittisiä RCE-haavoittuvuuksia ja ei ilmoitettuja nollapäiviä	200 haavoittuvuutta, joista 33 kriittisiä ja kuusi nollapäivää	570 haavoittuvuutta, joista 59 kriittisiä ja kolme nollapäivää
Oracle	35 uutta korjausta ensimmäisessä kohdennetussa CSPU-päivityksessä	245 uutta korjausta CSPU-päivityksessä	1 449 uutta korjausta laajassa neljännesvuosittaisessa CPU-päivityksessä
Linux-ekosysteemi	Päivittyvässä Linux Patch Wednesday -aineistossa 1 706 haavoittuvuutta; ensimmäinen julkaistu kooste sisälsi 1 638 haavoittuvuutta, joista 474 Linux-kernelissä	1 888 haavoittuvuutta, joista 324 Linux-kernelissä	Kuukausi on vielä kesken; pelkästään 19.–20.7. julkaistiin yli 400 Linux-kernelin CVE-ilmoitusta noin vuorokaudessa

Microsoftin luvut perustuvat touko⁵-, kesä⁵- ja heinäkuun⁷ Patch Tuesday -koosteisiin. Oraclen luvut ovat yhtiön omista tiedotteista: toukokuu⁸, kesäkuu⁹ ja heinäkuu¹⁰. Oracle käynnisti toukokuussa uuden kohdennet-

tujen Critical Security Patch Update -päivitysten sarjan täydentämään neljännesvuosittaisia päivityksiä. Linux-luvut ovat riippumattomasta, eri jakelujen tietoturvatiedotteita kokoavasta Linux Patch

Wednesday¹¹ -aineistosta. Heinäkuun yli 400 CVE piikki¹² koski Linux-kernelin upstream-ilmoituksia, joten sitä ei pidä verrata suoraan aikaisempien kuukausien koko ekosysteemin lukuihin.

Mitä luvuista pitää päätellä?

Ensimmäinen väärä johtopäätös olisi se, että ohjelmistot olisivat yhtäkkiä muuttuneet valtavasti huonommiksi. Todennäköisempi selitys on, että olemme saaneet käyttöömmme aikaisempaa tehokkaamman ”mikroskoopin”. Tekoäly löytää vanhoista ja uusista ohjelmistoista virheitä, joita ihmiset, fuzzing-työkälut ja aikaisemmat koodianalysaattorit eivät löytäneet.

Toinen väärä johtopäätös olisi väittää, että tekoäly olisi löytänyt jokaisen taulukossa olevan haavoittuvuuden. Näin ei ole. Mukana on myös perinteisillä menetelmillä löydettyjä haavoittuvuuksia, kolmansien osapuolten komponentteja, aikaisempien korjausten muunnelmia ja päivitysten julkaisurytmeistä johtuvia piikkejä. Silti kehityksen suunta on selvä: löydämme jatkossa enemmän haavoittuvuuksia ja löydämme niitä nopeammin.

Hyökkääjät saavat saman teknologisen hyödyn. He voivat analysoida juuri julkaistun korjauksen, paikantaa muutetun koodin, päättellä alkuperäisen haavoittuvuuden ja tuottaa toimivan hyökkäyksen aikaisempaa nopeammin. Aikaisemmin organisaatiolla saattoi olla päiviä tai viikkoja aikaa. Jatkossa aikaa voi olla tunteja, pian minuutteja.

Haavoittuvuuksien hallinta ei ole enää kuukausittainen huoltotoimi

Monessa organisaatiossa tietoturvapäivityksiä käsitellään edelleen teknisenä, jopa mekaanisena ylläpito-tehtävänä: päivitykset tarkistetaan tiettynä päivänä, testataan, viedään seuraavaan huoltoikkunaan ja raportoidaan lopuksi. Tämä toimintamalli on ehdottomasti jatkossa liian hidas! Haavoittuvuuksien hallinnan pitää muuttua jatkuvaksi, riskiperusteiseksi prosessiksi.

Organisaation on tiedettävä:

- Mitä laitteita, palveluita, sovelluksia, rajapintoja, pilviympäristöjä ja ohjelmistokomponentteja sillä on?
- Missä niitä käytetään ja ovatko ne yhteydessä internetiin?
- Mitä tietoja ja toimintoja niiden kautta voidaan saavuttaa?
- Onko haavoittuvuudelle olemassa toimiva hyökkäyskoodi tai havaintoja aktiivisesta hyväksikäytöstä?
- Millaisia väliaikaisia suojaustoimia voidaan ottaa käyttöön ennen varsinaista korjausta?
- Kuka voi päättää palvelun rajoittamisesta tai pysäyttämisestä? Ja tämä kyky pitää olla 24/7 riippumatta siitä, onko johto tavoitettavissa vai ei.

Pelkkä CVSS-luku ei enää riitä. Priorisoinnissa tarvitaan tietoa palvelun kriittisyydestä, todellisesta altistumisesta, hyökkäyksen todennäköisyydestä, saatavilla olevista hyväksikäyttömenetelmistä ja mahdollisen vahingon laajuudesta. Tekoälyä tarvitaan yhdistämään nämä tietomassat. Ihmistä tarvitaan päättämään, minkä riskin organisaatio voi hyväksyä.

Joskus turvallisin ratkaisu on palvelun pysäyttäminen

Jos internetiin avoimessa palvelussa on vakava, kriittinen haavoittuvuus, korjausta ei ole ja hyökkäyksiä havaitaan jo maailmalla, palvelun pitäminen normaalisti käytössä voi olla huomattavasti vaarallisempaa kuin sen tilapäinen rajoittaminen tai pysäyttäminen. Pysäyttäminen ei saa olla automaattinen reaktio jokaiseen haavoittuvuuteen. Myös käyttökatko voi vaarantaa toiminnan jatkuvuuden, turvallisuuden, ihmisten terveyden tai lakisääteisten palvelujen saatavuuden.

Päätös pitää tehdä vertaamalla kahta riskiä:

- Mitä tapahtuu, jos palvelu pysäytetään?
- Mitä tapahtuu, jos palvelu murretaan?

Tilapäinen, hallittu käyttökatko voi joskus olla paras jatkuvuutta turvaava ratkaisu. Hallittu katko kestää ehkä tunteja. Vakavan tietomurron selvittäminen, järjestelmien uudelleenrakentaminen, tietojen palauttaminen, asiakkaille ilmoittaminen ja luottamuksen korjaaminen voivat kestää kuukausia ja maksaa miljoonia euroja.

Jos korjausta ei ole saatavilla, vaihtoehtoja voivat olla esimerkiksi palvelun irrottaminen internetistä, haavoittuvan toiminnon poistaminen käytöstä, protokollan tai liikenteen estäminen, käyttöoikeuksien rajoittaminen, verkkosegmentointi, WAF-tai IPS-suojaus sekä tehostettu lokitus ja valvonta. Näiden toimien pitää kuitenkin olla ennalta suunniteltuja. Keskellä kriisiä ei pitäisi ensimmäistä kertaa selvittää, kuka saa pysäyttää organisaation kriittisen palvelun.

Mikä on lopputulos? Tietomurtojen määrä tulee kasvamaan

On käytännössä varmaa, että tekoäly lisää hyökkäysyritysten määrää. Tekoäly alentaa kustannuksia, automatisoi tiedustelua, etsii heikkoja kohtia, muokkaa hyökkäyksiä kohteen mukaan ja mahdollistaa useiden haavoittuvuuksien ketjuttamisen.

On myös erittäin todennäköistä, että onnistuneiden tietomurtojen määrä kasvaa ainakin lähivuosina. Kaikki organisaatiot eivät pysty päivittämään järjestelmiään riittävän nopeasti. Osa ei edes tiedä, missä kaikkialla haavoittuvaa komponenttia käytetään. Erityisen suuri riski liittyy vanhoihin järjestelmiin, räätälöityihin sovelluksiin, teollisuusympäristöihin, toimitusketjuihin ja ohjelmistoihin, joiden valmistajan tuki on päättynyt.

Tietomurrot syntyvät harvoin yhden virheen seurauksena. Tekoäly on erityisen tehokas etsimään ketjuja: pieni tietovuoto yhdistetään puutteelliseen tunnistamiseen, väärään asetukseen, liian laajoihin käyttöoikeuksiin ja lopulta varsinaiseen haavoittuvuuteen. Hyökkääjän ei tarvitse murtaa organisaation vahvinta kohtaa. Riittää, että tekoäly löytää heikoimman lenkin. Jos lenkki ei ole sinun organisaatiossa, se voi tunnistaa käytössäsi olevista palveluista ja toimittajista toimitusketjukokonaisuuden ja hakea sieltä kuuluisan heikoimman lenkin.

Uusista ohjelmistoista voidaan rakentaa aikaisempaa turvallisempia

Tässä kehityksessä on onneksi myös erittäin myönteinen puoli. Jos tekoäly pystyy etsimään haavoittuvuuksia valmiista ohjelmistoista, sitä voidaan käyttää myös ennen ohjelmiston julkaisemista. Tekoäly voi tarkastaa koodia, analysoida arkkituhtuuria, muodostaa uhkamalleja, tunnistaa vaarallisia riippuvuuksia, tuottaa testitapauksia ja etsiä erilaisia tapoja murtaa sovellus.

Tavoitteena ei voi olla täysin tekoälyhyökkäyksen kestävä ohjelmisto. Täydellistä, 100 % turvallisuutta ei nimittäin ole. Voimme kuitenkin rakentaa ohjelmistoja, joita tekoälyavusteisen hyökkääjän on merkittävästi vaikeampi murtaa. Tämä edellyttää turvallisuutta jo suunnitteluvaiheessa:

1. Turvalliset oletusasetukset ja mahdollisimman pieni hyökkäyspinta.
2. Vähemmän oikeuden periaate, vahva tunnistaminen ja toimintojen eriyttäminen.
3. Muistiturvallisten ohjelmointikielten käyttäminen aina, kun se on tarkoituksenmukaista.
4. Ohjelmistokomponenttien ja riippuvuuksien tunteminen SBOM-tietojen avulla.
5. Jatkuva tekoälyavusteinen koodin, rajapintojen ja muutosten tarkastus.
6. Lokitus, valvonta ja mahdollisuus havaita myös onnistunut hyökkäys.
7. Kyky päivittää ja tarvittaessa poistaa haavoittuva toiminto nopeasti käytöstä.
8. Ihmisen suorittama kriittisten havaintojen, korjausten ja päätösten arviointi.

Tekoälyn pitää siis olla mukana sekä punaisessa että sinisessä joukkueessa: yrittämässä murtaa järjestelmä ennen rikollista ja auttamassa puolustajia korjaamaan löydetty heikkoudet.

Muutos ulottuu kaikkien digitaaliseen turvallisuuteen

Riskienhallinta

Perinteinen riskirekisteri vanhenee helposti jo ennen seuraavaa kokousta. Tekoäly voi seurata uhkatietoa, haavoittuvuuksia, omaisuustietoja, toimitusketjuja ja toimintaympäristön muutoksia jatkuvasti. Se voi muodostaa uusia riskiskenaarioita, tunnistaa riippuvuuksia ja arvioida, miten yhden toimittajan tai komponentin häiriö vaikuttaa muihin palveluihin. Ihminen määrittää edelleen riskin merkityksen, hyväksyttävyyden ja tarvittavat toimenpiteet. Tekoäly ei saa yksin päättää, millainen riski ihmisille, yhteiskunnalle tai organisaatiolle on hyväksyttävä.

Toiminnan jatkuvuus ja varautuminen

Tekoäly voi auttaa tunnistamaan kriittiset riippuvuudet, simuloimaan

häiriötilanteita, laatimaan harjoituksia ja päivittämään toimintaohjeita havaintojen perusteella. Se voi myös tukea häiriötilanteen johtamista muodostamalla nopeasti tilannekuvaa, arvioimalla vaihtoehtoja ja tunnistamalla päätösten mahdollisia seurauksia. Samalla pitää varautua itse tekoälypalvelujen häiriöihin, virheellisiin vastauksiin, manipuloituihin lähtötietoihin ja tilanteisiin, joissa tärkeää palvelua ei voida käyttää. Myös tekoällylle tarvitaan jatkuvuussuunnitelma ja vaihtoehtoinen toimintatapa.

Tietoturva

Tekoälyä tarvitaan haavoittuvuuk-sien etsimiseen, hyökkäyspintojen kartoittamiseen, lokien analysointiin, poikkeamien tunnistamiseen, tietojenkalastelun torjuntaan, haittaohjelmien tutkimiseen ja tapahtumien priorisointiin. Turvallisuusvalvomon tehtävä ei enää ole vain havaita yksittäisiä hälytyksiä. Sen pitää pystyä tunnistamaan tekoälyn avulla nopeasti muuttuvia hyökkäysketjuja. Samalla tekoälyjärjestelmät muodostavat uuden hyökkäyspinnan. Mallit, agentit, työkalut, laajennukset, syötteet, muistot, käyttöoikeudet ja niiden käsittelemät tiedot pitää suojata kuten muutkin kriittiset järjestelmät.

Tietosuoja

Tekoäly voi auttaa tunnistamaan henkilötietoja, ylläpitämään käsitteilytoimien kuvauksia, arvioimaan tietosuojavaikutuksia, valvomaan säilytysaikoja ja havaitsemaan poikkeavaa tietojen käyttöä. Mutta tekoäly voi myös päätellä näennäisesti harmittomista tiedoista erittäin arkaluonteisia asioita. Se voi yhdistää hajallaan olevia tietoja, tunnistaa ihmisiä anonymisoiduista aineistoista tai levittää henkilötietoja hallitsemattomasti agenttien ja integraatioiden välillä. Tämä on yksi esimerkki, joka on erityisen huolestuttava, meidän ihmisten todella kehittynyt profiointi.

Tietosuojassa ei jatkossa riitä kysymys siitä, mitä tietoja järjestel-

mään tallennetaan. On kysyttävä myös, mitä tekoäly pystyy niiden perusteella päättämään, kenelle se voi tiedot välittää ja millaisia toimia se voi käynnistää.

Mitä organisaation pitää tehdä nyt?

Ensimmäinen askel ei ole ”mennä kauppaan” ostamaan uusi tekoälypalvelu. Ensimmäinen askel on tunnistaa, missä turvallisuustyössä ihminen on jo häviämässä nopeudessa, mittakaavassa tai havaintokyvyssä.

Sen jälkeen organisaation pitää:

1. rakentaa ajantasainen laite-, palvelu-, ohjelmisto- ja riippuvuusluettelo
2. ottaa tekoäly käyttöön haavoittuvuuksien, uhkien ja poikkeamien analysoinnissa
3. siirtyä kuukausittaisesta päivitysrytmistä jatkuvaan riskiperusteiseen haavoittuvuuksien hallintaan
4. määrittää korjausajat eri riskitasoille ja valvoa niiden toteutumista
5. sopia ennalta, milloin haavoittuvaa palvelua rajoitetaan tai se pysäytetään
6. harjoitella tilannetta, jossa kriittiseen palveluun ei ole saatavilla korjausta
7. käyttää tekoälyä uusien ohjelmistojen uhkamallinnuksessa, testauksessa ja koodikatselmoinnissa
8. pitää ihminen vastuullisena kriittisistä päätöksistä ja tekoälyn tuottamien havaintojen laadusta.

Tekoäly ei poista turvallisuusammattilaisten tarvetta. Päinvastoin: se lisää osaavien ihmisten tarvetta, koska löydöksiä, korjauksia ja päätöksiä tulee enemmän kuin koskaan aikaisemmin. Turvallisuus ei edelleenkaan synny teknologiasta, vaan ihmisistä. Mutta jatkossa turvallisuutta ei enää voida rakentaa ilman tekoälyä.

LÄHTEET

- 1 Anthropic: Evaluating and mitigating the growing risk of LLM-discovered 0-days: <https://www.anthropic.com/research/zero-days>
- 2 Microsoft: Defense at AI speed: <https://www.microsoft.com/en-us/security/blog/2026/05/12/defense-at-ai-speed-microsofts-new-multi-model-agentic-security-system-tops-leading-industry-benchmark/>
- 3 Microsoft: Evolving Windows vulnerability management: <https://blogs.windows.com/windowsexperience/2026/07/09/evolving-windows-vulnerability-management-to-meet-the-speed-of-ai-powered-discovery/>
- 4 OpenAI: Daybreak: <https://openai.com/index/daybreak-securing-the-world/>
- 5 <https://cybersecuritynews.com/microsoft-patch-tuesday-may-2026/>
- 6 <https://www.bleepingcomputer.com/news/microsoft/microsoft-june-2026-patch-tuesday-fixes-6-zero-days-200-flaws/>
- 7 <https://www.bleepingcomputer.com/news/microsoft/microsoft-july-2026-patch-tuesday-fixes-massive-570-flaws-3-zero-days/>
- 8 <https://www.oracle.com/security-alerts/cspumay2026.html>
- 9 <https://www.oracle.com/security-alerts/cspujun2026.html>
- 10 <https://www.oracle.com/security-alerts/cpujul2026.html>
- 11 <https://github.com/leonov-av/linux-patch-wednesday>
- 12 <https://cybersecuritynews.com/linux-patches-400-kernel-vulnerabilities/>

KIRJOITTAJA:



KIMMO ROUSKU

Tietoturva ry,
hallituksen jäsen



➤ RISTO RAJALA
& PETER SUND

Toimintavarmuuden ja luotettavuuden merkitys korostuvat entisestään kyberturvallisuuden muutostrendien voimistuessa

Edistyneimpien tekoälymallien kiihtyvä kehitys ja niiden vaikutukset kyberturvallisuuteen ovat herättäneet voimakasta keskustelua, sillä mallien on väitetty löytäneen jopa kymmeniä tuhansia haavoittuvuuksia kriittisistä ohjelmistoista. Yksinkertaisempienkin tekoälytyökalujen leviämisen myötä kes-

kimääräinen aika haavoittuvuuden löytämisestä sen hyväksikäyttöön on lyhentynyt merkittävästi, käytännössä muutamista päivistä jopa tunteihin. Tekoälymallien kehitymisestä ja yleistymisestä huolimatta kyberturvallisuuden perusfundamentit eivät kuitenkaan ole muuttuneet tai muuttumassa. Arkipäivi-

sen digitaalisten riskien hallinnan ja siihen liittyvien toimien, kuten käytössä olevien laitteiden ja ohjelmistojen inventoinnin, haavoittuvuuksien systemaattisen päivitys- ja korjausprosessin, identiteetin ja pääsynhallinnan, verkon segmentoinnin sekä jatkuva valvonnan ja lokien seurannan merkitys organisaatioiden ja

yhteiskuntien kyberturvallisuuden ylläpitämisessä korostuvat entisestään. Tekoälyohjelmistojen kyberturvallisuusvaikutukseen varautumisessa onkin kyse ennen kaikkea korjaustoimien nopeudesta, ja automatisoinnista sekä skaalaamisesta.

Nykyhetken edistyneimmät tekoälymallit on kehitetty poikkeuksetta Suomen ja Euroopan Unionin (EU) ulkopuolella, josta niitä myös hallinnoidaan. Tämä, yhdistettynä muihin kriittisten digitaalisten palveluiden saatavuuteen ja toimitusvarmuuteen kohdistuneisiin huoliin on vaikuttanut voimakkaasti Euroopassa käytävään poliittiseen keskusteluun, ja vaatimukset digitaalisen suvereniteetin vahvistamisesta ovat korostuneet entisestään. Kyberturvallisuuden kannalta on kiistatta ongelmallista, että eurooppalaiset organisaatiot pääsevät hyödyntämään edistyneimpiä tekoälymalleja hyvin rajatusti, jos ollenkaan. Yhdysvaltojen poukkoileva, arvaamaton ja jopa vihamielinen politiikka on ollut omiaan heittämään bensaa liekkeihin. Kesäkuussa tehty päätös rajata Anthropicin Claude Fable 5 -mallin käyttöoikeus ainoastaan Yhdysvaltojen kansalaisille, sen oltua hetken saatavilla globaalisti, osoitti korutomasti EU:n haavoittuvan aseman, sekä riippuvaisuuden Yhdysvaltojen hallinnon vähenevästä hyväntahtoisuudesta. Vaikka rajoitus myöhemmin purettiin, on Yhdysvallat nyt viimeistään osoittanut, että sillä on tahto ja kyky rajoittaa lainkäyttövaltansa alla toimivien yritysten tarjoamien digitaalisten palveluiden saatavuutta EU-alueella.

Keskustelu EU:n digitaalisen suvereniteetin vahvistamisesta on jatkunut kiivaana. Unionin voimattomuus Yhdysvaltojen yksipuolisten vientirajoitusten edessä on ollut suuri järkytys monille poliitikoille. Vaikka edistyneimpien tekoälymallien saatavuuteen kohdistuvat huolet ovatkin dominoineet julkista keskustelua, suuremmassa kuvassa merkityksellistä on huomioida, että jopa yli 80 % EU:ssa käytettävistä digituotteista, -palveluista ja -infrastruk-

tuurista tulee unionin ulkopuolelta, minkä lisäksi eurooppalaiset yritykset käyttävät vuosittain 264 ja julkissektori arviolta ainakin 50 miljardia euroa ostoihin pääosin yhdysvaltalaisilta it-toimittajilta. EU:n teknologiapolitiikan suunta viekin vahvasti kohti kriittisimpien riippuvuuksien purkamista, sekä eurooppalaisten teknologioiden suosimista suvereniteetin nimissä. Kyberala ry puhuu kuitenkin digitaalisen suvereniteetin strategiasta autonomiainvointia painottaen, sillä koemme ”suvereniteetin” tässä kontekstissa terminologisesti ongelmallisena, eikä valtiolliseen suvereniteettiin verrattavan tilan saavuttaminen verkotuneessa digitaalisessa maailmassa ei ole realistista, eikä edes tavoiteltavaa. Strateginen autonomia, jossa riippuvuudet ovat hallinnassa, sen sijaan kuvaa selkeämmin tasapainoista tavoitetilaa. Toimiala korostaa erityisesti digitaalisten palveluiden toimitusvarmuuden ja jatkuvuuden turvaamista sekä toimitusketjuissa mukana olevien toimijoiden luotettavuuden merkitystä.

EU:n teknologia-suvereniteetin paketti

EU:n teknologiasuvereniteettipaketti julkaistiin kesäkuussa 2026. Se sisältää Pilvi- ja tekoälykehitysasetuksen eli CADA:n, uuden sirusäädöksen (2.0), avoimen lähdekoodin strategian sekä tiekartan tekoälyn ja digitalisaation roolista energiasektorilla. Paketin yhteinen tavoite on vähentää kriittisiä riippuvuuksia EU:n ulkopuolisista teknologioista ja vahvistaa Euroopan kilpailukykyä, toimintavarmuutta ja strategista autonomiainvointia. Kyberturvallisuusteollisuuden näkökulmasta CADA on paketin tärkein osa, joskaan avoimen lähdekoodiin liittyvän toiminnan strategista hallintaa ei tule väheksyä. CADAn tavoitteena on lisätä Euroopan pilvi- ja tekoälykapasiteettia, luoda pilvipalveluiden suvereniteettikehys, asettaa julkiselle sektorille uusia hankintavelvoitteita

sekä perustaa EuroCloud-federaatio ja yhteishankintakehys. Ehdotus on lähtökohtaisesti oikeansuuntainen, koska se pyrkii rakentamaan strategista autonomiainvointia ennen kaikkea kilpailukykyyn, investointien ja eurooppalaisen osaamisen kautta. Sääntelyvaatimusten tulee kuitenkin olla hyvin tarkkarajaisia ja riskiperusteisia.

CADA:n suvereniteettikehys ohjaisi julkisen sektorin pilvihankintoja neljän ”luotettavuustason” avulla. Alimmalla tasolla riittäisi EU-alueella tapahtuva tietojenkäsittely ja itsearviointi, kun taas ylemmillä tasoilla vaadittaisiin tiukempia ehtoja esimerkiksi kolmansien maiden vaikutusvallalle, omistukselle, toimitusketjun läpinäkyvyydelle ja auditoinnille. Tämä riskiperusteinen malli on parempi kuin jäykät yhden koon suvereniteettivaatimukset. PK-yritysten kannalta on tärkeää, että kerran saatu tunnistaminen kelpaa koko EU:ssa ilman erillisiä kansallisia hyväksyntöjä. Keskeiset markkinoillepääsyn kriteerit tulisi kuitenkin kirjata itse asetukseen, eikä niitä tulisi voida muuttaa olennaisesti delegoiduilla säädöksillä ilman riittäviä siirtymäaikoja. Suurin käytännön riski liittyy siihen, että luotettavuustasot 2–4 nojaavat EU:n pilvipalveluiden kyberturvallisuussertifiointikehykseen EUCS:ään, jota ei ole vielä saatu valmiiksi. Jos EUCS viivästyy, väliaikaiset kansalliset ratkaisut voivat sirpaloida EU:n sisämarkkinaa. Suomen kannalta on tärkeää, että kansalliset arviointikäytännöt, kuten pilvipalveluiden KriPa, tunnustetaan siirtymäkaudella. EUCS:lle tulisi asettaa selkeä määräaika ennen kuin ylempien tasojen hankintavelvoitteet tulevat voimaan. Sertifikaattien ja auditointien tulisi myös kelvata todisteeksi NIS2- ja CRA-vaatimusten täyttämiseksi, jotta yrityksille ei synny päällekkäisiä velvoitteita.

Esityksen tunnustamis- ja auditointimenettelyä on kevennettävä. Kansallinen arviointi, jäsenvaltioiden kuuleminen, mahdolliset vastalauseet ja komission päätös voivat

yhdessä tehdä prosessista hitaan ja vaikeasti ennakoitavan. Tämä olisi erityisen ongelmallista pk-yrityksille ja nopeasti kehittyville palveluille. Menettelylle tarvitaankin siksi sitova kokonaismääräaika. Myös auditointikapasiteettia on rakennettava ajoissa, jotta vuosittaiset auditoinnit eivät muodostu pullonkaulaksi. Suomessa toimivaltaiseksi viranomaiseksi nimettäneen Traficomin Kyberturvallisuuskeskus, mikä edellyttäne edelleen viranomaisresurssien kohdentamista – osin ehkä jostain muusta luopumalla. Samalla on varmistettava, että seuraamusjärjestelmä on EU-tasolla yhdenmukainen. Hankintavelvoitteissakin on varmistettava oikeasuhtaisuus. Multi-vendor- ja multicloud-strategioiden huomiointi on myönteistä, mutta komission ei tulisi voida ohittaa jäsenvaltion omaa riskiarviota kansalliseen turvallisuuteen liittyvissä kysymyksissä. Myös 12 kuukauden siirtymäaika pakolli-

selle pilvimigraatiolle voi olla suu- rissa julkishallinnon järjestelmissä epärealistinen. Näin laaja markkinainterventio on tunnustettava palveluiden aito saatavuus ja poikkeusperusteiden tulee olla selkeitä. On varmistettava, ettei CADA luo päällekkäisyyksiä NIS2:n, CRA:n, KriPan tai tiedonhallintalain kanssa.

CADA voi avata uusia liike- toimintamahdollisuuksia pilvi- ja tekoälypalveluissa, arviointi- ja auditointipalveluissa, kyberturval- lisuuden testausympäristöissä, kriit- tisen infrastruktuurin palveluissa sekä yhteishankinnoissa. Erityisesti tavoite ohjata osa hankinnoista inno- vatiivisille pk-yrityksille on myön- teinen, jos siihen liittyvä raportointi ja muu hallinto pysyy kevyenä. Samalla eurooppalaista lisäarvoa koskevien hankintakriteerien on oltava varovaisia: niiden ei tule syr- jiä suomalaisia vientiyrityksiä, jotka toimivat globaaleissa arvoketjuissa, ja WTO-velvoitteet on myös huo- mioitava.

Esityksen mukainen EuroCloud- federaatio voi tehostaa julkisen sek- torin kapasiteetin käyttöä, mutta se ei saa vääristää markkinoita. Viran- omaisten ei tule tuottaa palveluja, joita markkinat voivat tarjota. Kapa- siteetin jakaminen on rajattava aidon ylikapasiteetin hyödyntämiseen, ja samoja turvallisuus- ja vakuutta- mistasovaatimuksia on sovellettava myös jaettuihin palveluihin. Avoi- men lähdekoodin suosiminen on kannatettavaa vain, jos turvallisuus, ylläpito ja elinkaarivastuut saadaan hallittua. Kolmansia maita koskeva tunnustamismekanismi on tärkeä joustomekanismi, koska se mahdol- listaa vaikuttavan yhteistyön luo- tettavien kumppanimaiden kanssa. Kriteerien on kuitenkin edelleen oltava selkeät, ja mahdollisille peru- tuksille on säädettävä siirtymäajat. Kokonaisuutena CADA voi vahvistaa eurooppalaista pilvi- ja tekoälymark- kinaa, jos se toteutetaan ennakoita- vasti, riskiperusteisesti ja yritysten kilpailukykyä tukevalla tavalla.

Kyberturvallisuuden ja tekoälyn tiekartta

Pian suvereniteettipaketin jälkeen komissio julkaisi heinäkuussa 2026 kyberturvallisuuden ja tekoälyn tie- kartan. Kyseessä on ei-lainsäädän- nöllinen suunnitelma siitä, miten EU vastaa tekoälyn aiheuttamiin kyber- turvallisuusriskeihin ja hyödyntää sen mahdollisuuksia kyberturval- lisuuden vahvistamiseen. Tiekar- tan tavoitteena on tehdä edistynyt tekoäly turvallisesti saavutettavaksi kyberturvallisuuskäyttöön, valmis- taa eurooppalaiset organisaatiot tekoälyllä tehostettuihin uhkiiin ja skaalata eurooppalaisia tekoälypoh- jaisia kyberratkaisuja.

Tiekartassa linjataan arviointi- mekanismin perustamisesta tekoäly- malleille komission tekoälytoimiston yhteyteen, jonka tarkoituksena olisi muun muassa arvioida tekoälymal- lien kyberturvallisuusvaikutuksia ennen niiden tuloa markkinoille. Tiekartan mukaan Komissio ja Euroopan kyberturvallisuusvi- rasto (ENISA) myös valmistelevat vuoden 2026 loppuun mennessä rakenteellisen suunnitelman, jonka puitteissa eurooppalaiset viranomai- set, kriittisen infrastruktuurin toi- mijat, kyberturvallisuusyritykset ja tutkijat voisivat saada jäsennel- lyn pääsyn edistyneimpiin tekoäly- malleihin. On kuitenkin toistaiseksi epäselvää, miten edistyneimpiä teko- älymalleja hallinnoivat kolmansista maista käsin toimivat yritykset näi- hin ehdotuksiin suhtautuvat, tai ovatko ne ylipäättään kiinnostuneita yhteistyöstä. ENISA ja komission Tiede- ja tietopalvelu valmistelevat myös testausalustaa, jossa yritykset ja tutkimuslaitokset voivat kokeilla tekoälypohjaisia kyberturvallisuus- ratkaisuja valvotuissa ympäristöissä ennen käyttöönottoa. Tämä voi syn- nyttää liiketoimintaa esimerkiksi kyberharjoitusympäristöjä ja arvi- ointilaitoksia ylläpitäville yrityksille.

Tiekartan toinen kokonaisuus koskee varautumista. ENISAn on tarkoitus julkaista ohjeistus teko- älyllä tehostettuja uhkia vastaan

suojaudumisesta ja tekoälyn turval- lisesta käytöstä kyberturvallisuus- den operatiivisessa toiminnassa. Samalla tiekartta linjaa koordinoi- dun haavoittuvuuksien ilmoitta- misen käytäntöjen päivittämisestä EU-instituutioiden, jäsenvaltioiden ja teollisuuden välisessä yhteistyössä, koska tekoäly voi lisätä automatisoi- tuja ja heikkolaatuaisia haavoittuvuu- silmoituksia. EU käynnistää myös kriittisen avoimen lähdekoodin resi- lienssikampanjan, jossa kartoitetaan tärkeitä avoimen lähdekoodin kom- ponentteja ja tuetaan niiden ylläpi- toa ja turvallisuutta.

Kolmas kokonaisuus liittyy investointeihin ja osaamiseen. EU aikoo käynnistää vuoden 2026 lopussa Kyberkompetenssikeskuk- sen (ECCC) kautta Grand Challenge -kilpailun tekoälyavusteiseen haa- voittuvuuksien korjaamiseen sekä hyödyntää tekoälytehtaita, lasken- takapasiteettia, koulutusmoduuleja ja päivitettyä kyberturvallisuusosaa- misen viitekehystä. Haasteen tarkka muoto ja sisältö ovat vielä epäselviä, mutta se tarjoaa varmasti suomalai- selle kyberturvallisuusteollisuudelle rahoitus- ja liiketoimintamahdolli- suuksia.

Luotettavien toimittajien merkitys korostuu

Suvereniteettiin ja strategiseen auto- nomiaan liittyvä julkinen keskustelu on kuluneen vuoden tapahtumien valossa ymmärrettävästi keskittynyt EU:n ulkopuolisten maiden lainkäyt- tövallan alaisuudessa toimivien yri- tysten tuottamien digitaalisten pal- veluiden saatavuuteen ja toimitus- varmuuteen. Kolmannen osapuolen riskin osuus kyberturvallisuuspoik- keamissa kasvaa jatkuvasti ja toimi- tusketjun heikoimman lenkin muo- dostavan yhä suuremman osan koko- naisriskistä. Kyberturvallisuuden näkökulmasta on kuitenkin ehdot- toman oleellista kiinnittää huomi- oita myös toimitusketjuissa mukana olevien EU:n ulkopuolisista maista

käsin tuotettujen ohjelmistojen ja komponenttien luotettavuuteen ja niissä mahdollisesti piileviin riskei- hin. Komponentin halvan hinnan taustalla voi olla puutteellinen laa- dunvalvonta tai pahimmillaan jopa tarkoituksellinen ohjelmistohaavoit- tuvuus, jota ei havaita normaalissa tarkastuksessa – tutkimuksissa on löydetty takaportteja esimerkiksi kiin- nalaisvalmisteisista aurinkopanee- leista ja monista muista laitteista – piilotetuista ja lainvastaisista data- virroista puhumattakaan. Edullisin hinnoin toimivat toimittajat usein välttävät tai eivät läpäise riippumat- tomia tietoturva-auditointeja, jolloin haavoittuvuudet ja komponenttien alkuperä jäävät todentamatta. Halpa hinta saatetaan saavuttaa usein pit- kän ja hämärän alihankintaketjun kautta, jolloin lopullinen ostaja ei tiedä, kuka komponentit todellisuu- dessa on valmistanut tai koodannut.

Osa toimitusketjuun liittyvistä riskeistä saattaa liittyä suoraan toi- mittajayrityksen kotimaahan, esi- merkiksi sen lainsäädännön tai poliittisen järjestelmän tai toimin- tatapojen vuoksi. Autoritäärisesti johdetuissa maista, kuten Kiinasta, käsin toimivat yritykset ovat lain- nojalla velvoitettuja luovuttamaan dataa tai pääsyoikeuksia valtion viranomaisille ilman että asiakas saa siitä tietoa. Laitteet ja ohjelmis- tot myös vaativat jatkuvia päivityk- siä valmistajalta, ja jos toimittaja on autoritäärisesti johdetun kolmannen valtion vaikutuksen alainen, päivi- tyskanava itsessään on mahdollinen hyökkäysreitti. Geopolitiikan tasolla kriittisen infrastruktuurin riippu- vuus yksittäisestä autoritäärisestä valtiosta antaa kyseiselle valtiolle mahdollisuuden käyttää toimitus- ketjua painostuskeinona kriisitilan- teissa, joka voi ilmetä esimerkiksi toimitusten katkaisuna tai etäkäy- tön hyödyntämisenä.

EU:n lainsäädäntöprosessissa valmistellaan parhaillaan merkit- täviä toimia toimitusketjuriskien hillitsemiseksi. Vaikka ne eivät komission esittämään suvereni- teettipakettiin muodollisesti kuulu,



saattaa niiden vaikutus tosiasiallisesti olla jopa kesäkuussa esitettyjä toimia merkittävämpi. Komissio antoi keväällä 2026 lakiehdotuksen koskien kyberturvallisuusasetuksen (CSA2) kokonaisuudistusta. Ehdotuksen tavoite on luoda vahvempi ja yhtenäisempi EU:n kyberturvallisuusjärjestelmä uudistamalla ENISA:n toimivaltuudet, modernisoimalla ja laajentamalla kyberturvallisuushyödykkeiden sertifiointijärjestelmä. Esityksen merkittävin osa on EU-tason mekanismin perustaminen ICT-toimintusketjujen riskien hallintaan, joka rakentuisi EU-tasoiselle, riskiperusteiselle ja teknologianeutraalille kehiksellä, jonka tavoitteena on tunnistaa kriittiset ICT-komponentit ja niihin liittyvät toimitajariippuvuudet sekä arvioida näihin liittyvät ei-tekniset kyberriskit kuten kolmansien maiden lainsäädännöllinen tai geopolitiinen vaikutusvalta. Vaikka myös jo aiemmin hyväksytty NIS2-direktiivi ja erityisesti kyberkestävyysäädös puuttuvat osaltaan toimitusketjuris-keihin, mekanismi täyttää esitetyssä muodossaan aukon, joita nämä kaksi säädöstä eivät voi kattaa. Myös komission ehdotus digitaalisia verkkoja koskevaksi asetukseksi (DNA) tulee osaltaan vaikuttamaan kokonaisuuteen. Asetusehdotuksen tavoitteet digitaalisten verkkojen turvallisuuden, toimintavarmuuden ja häiriönsietokyvyn vahvistamiseksi ovat kannatettavia elinkeinoelämän digitalisaatiolle sekä Euroopan kilpailukyvyllä, mutta on tärkeää varmistaa, että sen turvallisuutta koskevat osiot tukevat investointeja ja innovaatioita eikä epävarmuutta tai päällekkäisiä velvoitteita lisätä jo valmiiksi laajasti säännellyssä ja riskiperusteisessa toimintaympäristössä. Samalla on varmistettava, että säännökset ovat saumattomasti yhteensopivia muun EU:n kyberturvallisuussäätelyn kanssa.

Euroopan kyber-turvallisuus riippuu teollisuuden menestyksestä

Kyberturvallisuudesta huolehtiminen on niin yritysten ja organisaatioiden kuin kokonaisten yhteiskuntienkin toiminnan kannalta välttämätöntä, ja sen merkitys jatkaa entisestään kasvuaan. Tekoälymallien kehitys ja leviäminen korostavat kyberturvallisuustoimien nopeuden ja skaalautumisen merkitystä, mutta pohjimmiltaan kyse on edelleen arkipäiväisestä digitaalisten riskien hallinnasta. Tilanteessa, jossa nopeus ratkaisee, on entistäkin tärkeämpää, että kyberturvallisuuden perustaso on yrityksissä ja organisaatioissa riittävä ja soveltuvalta osin automatisoitu, varsinkin kun kyse on yhteiskunnan kannalta kriittisistä toiminnoista. Tällä hetkellä jo pelkästään kyberturvallisuuslain soveltamisaloilla on arviomme mukaan yhteensä jopa yli miljardin euron investointivaje lain edellyttämään vaatimustasoon nähden. Siksi on tärkeää, että kyberturvallisuusinvestointien toteuttamiselle luodaan taloudellisia kannustimia, esimerkiksi toteuttamalla monivuotinen kyberturvallisuuden tukiohjelma tulevalla vaalikaudella.

Vahva ja kilpailukykyinen kyberturvallisuusteollisuus on tekoälyn kehityksen vaatiman kyberturvallisuuden tasonnoston edellytys niin Suomen kuin Euroopan tasolla. Kyberala ry tekee aktiivista vaikuttamistyötä Suomessa toimivan kyberturvallisuusteollisuuden toimintaedellytysten turvaamiseksi sekä liiketoimintamahdollisuuksien lisäämiseksi.

Vahva ja kilpailukykyinen kyberturvallisuusteollisuus on tekoälyn kehityksen vaatiman kyberturvallisuuden tasonnoston edellytys niin Suomen kuin Euroopan tasolla. Kyberala ry tekee aktiivista vaikuttamistyötä Suomessa toimivan kyberturvallisuusteollisuuden toimintaedellytysten turvaamiseksi sekä liiketoimintamahdollisuuksien lisäämiseksi.

KIRJOITTAJAT:



PETER SUND

Kyberala ry:n (FISC ry) toimitusjohtaja

Teknologiateollisuus ry



RISTO RAJALA

Kyberala ry:n (FISC ry) neuvonantaja

Teknologiateollisuus ry



Cyberwatch Finland

VIKKOKATSAUS

29/2026

Teemakatsaus

KYBERHYÖKKÄYSTEN PSYKOLOGINEN ULOTTUVUUS JA KYBERPSYKOLOGINEN SODANKÄYNTI





Johdanto

Kyberhyökkäysten psykologinen vaikutus koh-teisiin jää usein huomiotta. Julkinen keskustelu keskittyy yleensä varastettuihin tietoihin, lamau-tettuihin järjestelmiin ja taloudellisiin menetyksiin, mutta tutkimusnäyttö viittaa yhä enenevässä mää-rin siihen, että monien kyberhyökkäysten merkittä-vin ulottuvuus on usein juuri psykologinen. Tämä pätee erityisesti aktiivisten konfliktien aikana teh-

tyihin hyökkäyksiin, kuten Ukrainan ja Lähi-idän viimeaikaiset sodat ovat osoittaneet. Tässä katsa-uksessa selvitetään ensin, mitä kyberpsykologinen sodankäynti on ja miten se asettuu osaksi laajem-paa kognitiivisen sodankäynnin käsitettä. Sen jäl-keen tarkastellaan, miten sitä on käytetty käytän-nössä Ukrainan ja Venäjän sekä Iranin ja Israelin välisissä konflikteissa.



Mitä kyberpsykologinen sodankäynti on?

Kyberpsykologinen sodankäynti on helpointa hah-mottaa kognitiivisen sodankäynnin alalajiksi. Kogni-tiivisella sodankäynnillä tarkoitetaan sodankäynnin osa-aluetta, jonka tavoitteena on muokata vastusta-jan ajattelua. Käsitteillä on sama perimmäinen pää-määrä, minkä vuoksi ensin mainittua on perustel-tua pitää jälkimmäisen alalajina. Eroa ei kuitenkaan pidä häivyttää kokonaan. Kognitiivinen sodankäynti on huomattavasti laajempi käsite, joka toimii myös kybermaailman ulkopuolella – muun muassa perin-teisen propagandan, radio- ja televisiolähetysten sekä kasvokkain tapahtuvan vaikuttamisen kautta – kun taas kyberpsykologisella sodankäynnillä tarkoite-taan nimenomaan samojen kognitiivisten vaikutusten tavoittelua kyberkeinoin. Se on siis yksi kognitiivisen sodankäynnin välineistä, ei koko käsitteen synonyymi.

Tavanomaisessa kyberhyökkäyksessä psykologinen kuormitus on sivuvaikutus operaatiosta, jolla tavoitel-laan jotakin muuta, kun taas kognitiivisessa operaa-tiossa juuri kuormitus on itse tarkoitus. Alun perin fyysiseen häirintään tai tuhoamiseen tähdänneiden

operaatioidenkin merkittävimmät vaikutukset voivat kuitenkin olla lopulta psykologisia.

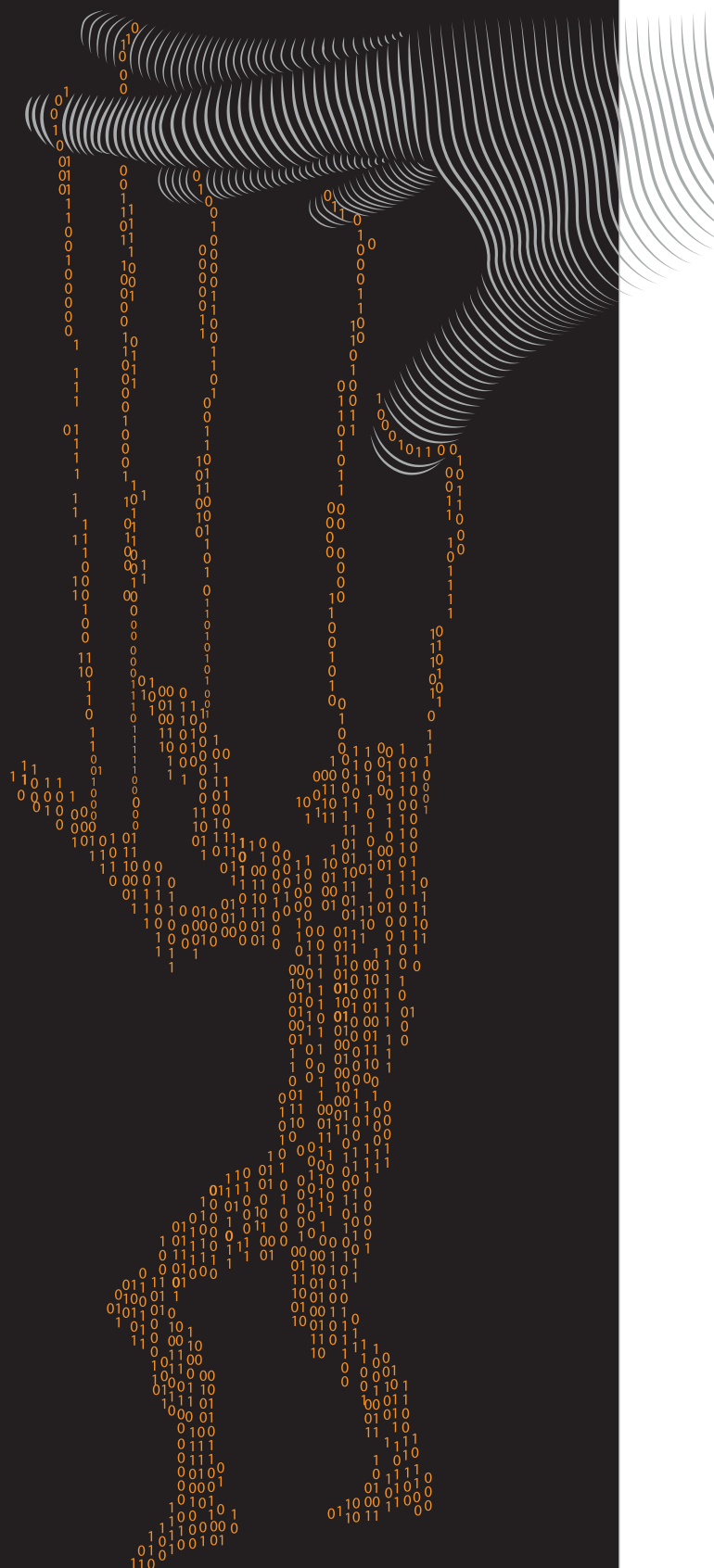
Psykologisia vaikutuksia on dokumentoitu hyvin monella tasolla. Tietomurron, kiristyshaittaohjel-man tai huijauksen kohteeksi joutuneiden yksilöiden osalta tutkimukset kuvaavat johdonmukaisesti ensijär-kytystä, jota seuraavat haavoittuvuuden ja loukatuksi tulemisen tunne, ahdistus, viha ja avuttomuus sekä jatkuva pelko identiteettivarkaudesta, talousrikoksen uhriksi joutumisesta tai kiristyksestä. Vakavimmissa tapauksissa trauma jää pysyväksi: lääkärit ovat rapor-toineet masennusta, ahdistuneisuutta, paniikkikoh-tauksia, traumaperäistä stressiä sekä ääritapauksissa itsemurhia, ja oireisiin liittyy usein unen ja syömisen häiriintymistä. Osa tutkijoista rinnastaa tietomur-ron uhrien kokemuksen suoraan trauman kokenei-den kokemukseen. Toistuva teema on luottamuksen rapautuminen: uhrien on jälkeensä vaikea uskoa tietojaan organisaatioiden haltuun, mikä voi vähitel-len johtaa eristäytymiseen. Suomen kontekstissa ken-

ties kuuluisin tapaus on Vastaamon tietomurto, jossa vietiin yli 30 000 asiakkaan potilas- ja henkilötietoja sekä henkilökunnan tietoja. Siitä on tehty myös psykologisia tutkimuksia, jotka avaavat aihetta lisää uhrien näkökulmasta kiinnostuneille.

Myös kohteeksi joutuneen organisaation sisällä kuormitus on raskaampaa kuin tavanomainen talous- ja mainehaittoihin keskittyvä tarkastelu antaa ymmärtää. Hyökkäyksen aikana ahdistus kärjistyy, päätöksenteko vaikeutuu paineen alla ja henkilöstö venyy kohtuuttoman pitkiin työpäiviin, mikä rasittaa sekä mieltä että kehoa. Tietomurron vahingossa aiheuttaneet työntekijät potevat usein syyllisyyttä, häpeää ja pelkoa, mikä heikentää työilmapiiiriä ja lisää työntekijöiden vaihtuvuutta. Erityisen kovilla ovat tietoturvaosikoiden selvittäjät: erään kyselyn mukaan noin 65 prosenttia heistä oli hakenut mielenterveysapua kyberturvallisuusosikoiden käsittelyn vuoksi.

Väestötasolla tutkimus osoittaa, että kyberhyökkäykset herättävät johdonmukaisesti pelkoa, ahdistusta ja vihaa sekä voimistavat uhkien ja riskien kokemusta. Altistuminen kyberterrorismille voi jopa synnyttää yhtä voimakkaita kielteisiä tunteita ja uhkakäsityksiä kuin perinteiset terrori-iskut. Eräässä kokeessa kohonneen kortisolitason avulla osoitettiin, että hyökkäyksen jälkeen voimakkaampaa stressiä kokevat ihmiset kannattavat muita todennäköisemmin kovan linjan vastatoimia. Strategisesti merkittäväksi ilmiön tekevät sen poliittiset seuraukset: ahdistus heikentää luottamusta hallintoon ja lisää kansalaisvapauksia kaventavan valtiollisen valvonnan kannatusta, ja laajalle levinnyt ahdinko voi synnyttää painetta sotilaalliseen vastaisuuteen, mikä sotii kybereskalaation hillitsemistä koskevia normeja vastaan.

Nämä havainnot selittävät myös kognitiivisten operaatioiden toimintamallin. Esimerkiksi kiristyshaittaohjelmaryhmät lietsovat pelkoa tietoisesti nimeämällä tahot, joille tieto murrosta voisi päättyä – valvontaviranomaiset, kilpailijat ja median. Näin ne herättävät huolta sääntelyseuraamuksista ja ilmoitusvelvollisuuksista sekä eristävät yksittäisiä järjestelmänvalvojia uhkaamalla ottaa yhteyttä heidän esihenkilöihinsä. Valtiollisella tasolla sama logiikka tiivistyy menetelmän ytimeksi: tunkeutuminen sairaalaan, sähköverkkoon tai vaalijärjestelmään aiheuttaa vain vähän fyysisistä vahinkoa, mutta viestii kyvykkyydestä, luo kaikkialle ulottuvaa turvattomuuden tunnetta ja nakertaa luottamusta instituutioihin, joiden varassa ihmiset elävät. Edellä kuvatut mitattavat psykologiset reaktiot – pelko, epäluottamus, kovien vastatoimien vaatiminen ja polarisaatio – ovat juuri niitä vaikutuksia, joita kognitiivisen operaation toteuttaja tavoittelee.



Ukraina: pelko aseena, resilienssi kilpenä

Ukrainan sodasta hahmottuva kaava on selkeä: kyberhyökkäysten sotilaallinen ja fyysinen vaikutus on jäänyt verrattain vähäiseksi, mutta ne ovat toimineet pitkälti psykologisen ja kognitiivisen painostuksen välineinä. Tulkinta toistuu analyttisessä kirjallisuudessa. Eyal Pinkon strategisen tutkimuksen Begin–Sadat-keskukselle (BESA) vuonna 2023 laatimassa analyysissa todettiin, että sodan ensimmäisenä vuonna kybertoimintaympäristön sotilaallinen vaikutus jäi mitättömäksi ja että osapuolet käyttivät kyberoperaatioita ensisijaisesti psykologiseen sodan käyntiin sekä yleisen mielipiteen muokkaamiseen.

Paras yksittäinen esimerkki on joulukuussa 2023 tehty hyökkäys Ukrainan suurinta teleoperaattoria Kyivstaria vastaan. Operaatio häiritsi noin 24 miljoonan liittymäasiakkaan matkapuhelin- ja internetyhteyksiä koko maassa ja lamautti ilmahälytysjärjestelmät Kiovan ja Sumyn alueilla. Ukrainan turvallisuuspalvelun kyberosaston johtajan mukaan hyökkäyksen tavoitteina olivat psykologisen iskun antaminen väestölle ja tiedustelutiedon kerääminen. Hän luonnehti sitä viestiksi ja varoitukseksi – ei vain Ukrainalle vaan koko läntiselle maailmalle – siitä, ettei kukaan ole todella suojassa. Juuri ilmahälytysten lamauttaminen muuttaa häirinnän kauhuksi, sillä se rapauttaa järjestelmää, jonka varassa ihmiset tuntevat olonsa turvallisiksi iskujen aikana ja niiden välissä. CrowdStriken arvio sijoitti tapauksen samaan kategoriaan: sen mukaan taustalla oli laajempi pyrkimys tukea psykologisia operaatioita, joilla heikennetään ja horjutetaan kansalaisten luottamusta valtion instituutioihin.

Laajempi kokonaiskuva tukee tätä tulkin-
taa. Chatham Housen tutkimuksessa Venäjän kyber- ja informaatio-
sodankäynnistä havaittiin, että
kyberhyökkäykset, joilla
ei ollut välitöntä taktista
tavoitetta, vaikuttivat
tavoittelevan Ukrainan
puolustajien pelotte-
lusta ja lannistamista.
Tutkimus dokumen-
toi myös tarkoituk-
sellista yhteensovitta-
mista kineettisten isku-
jen kanssa: syksyn 2022
kampanjassa Ukrainan
energiainfrastruktuurin



häirintään tarkoitetut kyberkyvyt sovitettiin operaatiivisella tasolla yhteen ohjusiskujen kanssa, jotta sekä fyysiset että psykologiset vaikutukset olisivat mahdollisimman suuria. Samaan joukkoon kuuluvat myös tietoja pysyvästi tuhoavat wiper-haittaohjelmakampanjat, kuten WhisperGate, HermeticWiper ja CaddyWiper, sillä niiden arvo on yhtä lailla kyvykkyydestä viestimisessä ja turvattomuuden lietsomisessa kuin tuhotussa datassa.

Toiminnassa on myös kohdennetumpi, henkilökoh-
tainen juonne: Solntsepekin kaltaiset haktivistiryhmät
ovat keskittyneet paljastamaan ukrainalaissotilaiden
henkilöllisyyksiä ja julkaisemaan heidän henkilö-
tietojaan, mikä on suoraa yksilöihin ja heidän perhei-
siinsä kohdistuvaa psykologista painostusta. Miguel
Alberto Gomezin ja Ryan Shandlerin Council on
Foreign Relations -ajatushautomolle laatimassa ana-
lyysissa esitetään, että sodan kyberhyökkäyksillä on
ollut merkittävä rooli yhteiskunnallisiin institu-
tioihin kohdistuvan luottamuksen rapauttamisessa,
vaikka merkittävät fyysiset vaikutukset ovat jääneet
saavuttamatta – ja juuri instituutioita kohtaan tun-
netun luottamuksen rapauttaminen on se vipu, jolla
sodan kannatusta pyritään murentamaan.

Tärkein huomio on kuitenkin se, ettei tavoiteltua vai-
kutusta ole merkittävässä määrin päässyt syntymään.
Ukrainalaisten resilienssi näyttää tylyttäneen Venä-
jän pyrkimykset. Useissa arvioissa päädytään siihen,
että Venäjän kyberkampanja epäonnistui strategisella
tasolla. Erään arvion mukaan epäonnistuminen johtui
ennen kaikkea Ukrainan tehokkaasta kyberresiliens-
sistä eikä pelkästään vahvasta puolustuksesta. Mie-
lialojen tasolla ukrainalainen yhteiskunta
on pysynyt pitkälti lujana: enemmistö
vastustaa yhä alueellisia tai poliit-
tisia myönnötyksiä Venäjälle,
vaikka sotaväsymys kasvaa.
Dynamiikka toimii myös
toiseen suuntaan: Ukrai-
nan vapaaehtoisen IT-ar-
meijan ja sen hyvin
näkyvien kampanjoi-
den arvioidaan vahvis-
taneen kotimaista tais-
telutahtoa ja viestineen
kansallisesta kriisinkes-
tävyvyydestä sekä kotimai-
selle että kansainväliselle
yleisölle.



Iran ja Israel: varjosota mielten hallinnasta

Iranin ja Israelin konfliktit havainnollistavat ilmiötä kenties vielä Ukrainaakin selvemmin, sillä niin monet operaatioista on rakennettu pelkän vaikutuksen sijaan nimenomaan viestin ympärille.

Israeliin kytketyllä puolella keskeinen toimija on Predatory Sparrow, farsinkieliseltä nimeltään Gonjeshke Darande. Analyytikot ja israelilainen media uskovat laajalti ryhmän liittyvän Israelin sotilastiedusteluun, joskaan Israel ei ole koskaan vahvistanut tätä, ja ryhmä itse kertoo koostuvansa iranilaisista hallinnonvastaaisista haktivisteista. Sen operaatioita leimaavat johdonmukaisesti mittava häirintä, tarkoituksellinen tietojen tuhoaminen ja provosoiva julkinen viestintä, jolla kohdetta pilkataan. Vuoden 2021 rautatiehyökkäyksessä haittaohjelma lamautti liikenteen ja esitti samalla pilkkaavia viestejä asemien näyttötauluilla. Samana vuonna tehdyssä polttoainejärjestelmään kohdistuneessa hyökkäyksessä, joka poisti käytöstä noin 80 prosenttia Iranin huoltoasemista, hyökkääjät kaappasivat lisäksi digitaalisia mainostauluja näyttääkseen korkeinta johtajaa arvostelevia viestejä. Vuonna 2022 terästehtaaseen kohdistuneen ja tulipalon aiheuttaneen hyökkäyksen jälkeen ryhmä puolestaan julkaisi tarkoituksella videomateriaalia vahingoista.

Mainostaulujen kaappaamisessa ja videomateriaalin julkaisemisessa on kyse yleisön huomiosta, ei sabotaasista. Kesäkuun 2025 kahdentoista päivän sodan aikana toiminta laajeni rahoitusjärjestelmään: ryhmä tuhosi valtio-omisteisen Bank Sepahin tietoja ja iski sitten Nobitex-kryptovaluuttapörssiin. Se tuhosi noin 90 miljoonan dollarin arvosta kryptovaluuttaa siirtämällä varat osoitteisiin, joihin kenelläkään ei ole pääsyä, ja julkaisi koko lähdekoodin; käytetty lompakko-osoite sisälsi Iranin vallankumouskaartille (IRGC) osoitetun solvauksen. Myös Iranin valtiontelevisio kaapattiin lähettämään materiaalia, jossa kehoitettiin kansannousuun. Analyytikot kuvaavat ryhmän menetelmää haittaohjelmien, tarkan ajoituksen ja psykologisen manipuloinnin yhdistelmäksi, jolla murennetaan vastustajan itseluottamusta.

Kahdentoista päivän sodassa kyberoperaatiot ja kineettiset operaatiot kietoutuivat entistä tiiviimmin yhteen. Kyberturvallisuusyhtiö ZENDATAN analyysin mukaan kyberhyökkäysten määrä kasvoi noin 700 prosenttia 48 tunnissa, yli sata Irania tukevaa haktivistiryhmää mobilisoitui Telegramissa ja useisiin hallintomyönteisiin iranilaisiin uutistoimistoihin murtauduttiin samanaikaisesti iskujen ensitunteina.

»

Iranin oma lähestymistapa nojaa paljon vahvemmin pelkoon ja seipitteeseen kuin fyysiseen vahinkoon – osin siksi, että maa pyrkii näin paikkaamaan tavanomaisen sotilaallisen voimansa puutteita. Foundation for Defense of Democracies -ajatushautomo kutsuu taktiikkaa mielikuvien hakkeroinniksi (engl. perception hacking): toiminnalla lietsotaan pelkoa ja vaikuttaa mielipiteisiin, usein liioittelemalla hyökkäyksen vaikutuksia tai keksimällä ne tyhjästä. Selkein esimerkki ovat Handala-ryhmän kymmenilletuhansille israelilaisille lähettämät uhkaavat tekstiviestit, joissa ryhmä väitti murtautuneensa Iron Dome -ilmatorjuntajärjestelmään ja varoitti, että vastaanottajilla oli vain sekunteja aikaa paeta. Todellisuudessa ryhmä oli ainoastaan murtautunut tekstiviestijärjestelmään lietsaakseen paniikkia. Toisella kertaa iranilainen uhkatoimija väitti kiristävänsä uhrejaan Nevatimin lentotukikohdan kameroista saadulla materiaalilla, vaikka vuodettu aineisto oli todellisuudessa peräisin kaupungista, jossa vain sattui olemaan samanniminen katu.

Microsoft on dokumentoinut, miten Iran verhoaa tällaiset operaatiot kostokertomuksiin ja tukeutuu yhä enemmän massoitain lähetettyihin tekstiviesteihin ja sähköposteihin, koska omaan puhelimeen tai sähköpostiin saapuva viesti iskee kovempaa kuin sosiaalisessa mediassa nähty. Vuosiin 2025–2026 mennessä toiminta oli muuttunut uhkaavammaksi ja paremmin ajoitetuksi: ohjusiskuja pakenevat israelilaiset saivat tekstiviestejä, jotka näennäisesti tarjosivat tietoa pommisuojaista mutta levittivätkin vakoiluohjelmaa. Kyseessä oli uudenlainen digitaalisen ja fyysisen hyökkäyksen yhdistelmä.

Selkein yksittäinen esimerkki puhtaasti psykologista vaikutusta varten suunnitellusta kyberhyökkäyksestä on BadeSaba-rukousovelluksen kaappaus. Tämä laajalti käytetty iranilainen uskonnollinen kalenterisovellus kaapattiin juuri sillä hetkellä, kun vuoden 2026 iskut alkoivat, ja sen kautta lähetettiin sotilashenkilöstölle loikkaamiseen kehoittavia viestejä. CSIS tulkitsee sen osoitukseksi siitä, miten Israel yhdistää kyber- ja vaikuttamisoperaatiot lietsaakseen hallinnonvastaista ajattelua. Ajoituksella pyrittiin kylvämään hämmennystä ilmahyökkäysten alkuhetkinä. Rukousovellus tavoittaa nimenomaan sen uskonnollisen, hallintoa tukevan väestöosan, jonka taistelutahto halutaan murtaa. Samaan aikaan Iranin IRNA-uutistoimisto ja hallinnon verkkosivustoja kaapattiin näyttämään hallinnonvastaista viestejä.

Aktiivisin iranilainen uhkatoimija Handala – jonka Yhdysvaltain oikeusministeriö on sittemmin virallisesti yhdistänyt Iranin tiedustelu- ja turvallisuusministeriöön – toimi murtautumalla pehmeisiin

kohteisiin ja ajoittamalla varastettujen tietojen julkaisun psykologisesti mahdollisimman tehokkaasti. Se levitti Israelin armeijan ja hallinnon henkilöstön henkilötietoja, vuoti miljoonien äänestäjien rekisteritietoja, julkaisi sähköverkkokarttoja ja esitti tappouhkauksia.

Kokonaisuutena Iranin ja Israelin väliset sodat vahvistavat keskeistä ajatusta: kumpikin osapuoli käyttää kyberkeinoja paljon enemmän mielten ja taistelutahdon muokkaamiseen kuin sodan ratkaisevana fyysisenä aseena. Se sopii itse asiassa varsin hyvin yhteen iranilaisen näkemyksen kanssa, jossa kyberpsykologinen sodankäynti hahmotetaan ”pehmeänä sotana” (jang-e narm). Sillä tarkoitetaan psykologista vaikuttamista ja propagandaa, joilla kohdemaata horjutetaan ilman aseellista voimankäyttöä.

Iran on muutenkin varautunut kognitiiviseen sodankäyntiin poikkeuksellisen hyvin. Tästä paras esimerkki on maan kansallinen tietoverkko (National Information Network, NIN). Kriisitilanteessa se voi korvata internetin: yhteydet ulkomaille katkaistaan, mutta kotimaiset palvelut jatkavat toimintaansa. Näin hallinto voi hallita koko digitaalista informaatiotilaa. Verkkoa voidaankin pitää suorana vastakeinona ulkomaisille kyberpsykologisille operaatioille.

Avoin analyttinen kysymys on, keskittykö kyberkeinojen psykologinen arvo kampanjan alkuvaiheeseen olosuhteita muokkaavaksi työkaluksi, vai voidaan niillä ylläpitää painetta läpi pitkän sodan. Vuoden 2026 sodassa Iranissa kyberkeinojen käyttö vaikuttamiseen ja painostukseen jatkui kuukausien ajan – ei kuitenkaan tasaisena virtana vaan tapahtumien laukaisemina sykäyksinä. SOCRadarin seurannassa havaittiin, että päivittäisten hyökkäysväitteiden määrä oli huipussaan pian suurten kineettisten iskujen jälkeen, ja vaikka monet väitteistä olivat liioiteltuja tai päällekkäisiä, niiden jatkuva virta synnytti psykologista painetta ja vahvisti ilmiötä mediassa.

Paras tämänhetkinen tulkinta, joka perustuu Iranin ja Israelin yleisöjä koskevien havaintojen riskiinvertailuun, on se, että kummallakin puolella vallitsi kriisinkestävyyden dynamiikka. Psykologiset kyberoperaatiot eivät siis juuri onnistuneet kääntämään suuren yleisön mielialoja haluttuun suuntaan, vaikka ne tuottivat selkeitä paikallisia vaikutuksia: pelkopiikkejä, jonkin verran onnistunutta värväystä ja Iranissa keinotekoisien yhtenäisyyden vaikutelman. Se on huomionarvoista, sillä johtopäätös on sama, johon tilanne Ukrainassakin viittaa: mitattavaa psykologista ahdinkoa kyllä syntyy, mutta resilienssi vaikeuttaa suurimman osan strategisesta vaikutuksesta.

Johtopäätökset

Kaikissa näissä konflikteissa toistuu yksi ja sama johtopäätös. Kyberhyökkäysten psykologinen ulottuvuus ei ole muihin päämääriin tähtäävien operaatioiden satunnainen sivutuote, vaan yhä useammin niiden ensisijainen tarkoitus, jonka varsinainen maali on ihmismieli. Kyberpsykologiset operaatiot tuottavat yksilötasolla luotettavasti suunnittelijoidensa tavoittelemat vaikutukset – pelkoa, ahdinkoa, loukatuksi tulemisen tunnetta ja rapautunutta luottamusta – ja ne voidaan kytkeä tiiviisti tavanomaiseen sotilaalliseen toimintaan. Yhteiskunnan tasolla ne ovat kuitenkin toistuvasti jääneet strategisesta tavoitteestaan, koska kansallinen kriisinkestävyys on yleensä väimentanut iskun ja koska kriisin yhteen kokoava vaikutus kääntää yleisen mielipiteen usein päinvastaiseen suuntaan. Tilannetta mutkistaa vielä se, että yksittäisen kyberoperaation osuutta on äärimmäisen vaikea erottaa kaikesta muusta, mitä käynnissä olevassa sodassa tapahtuu. Mieli voi olla hyökkäyksen varsi-

nainen maali, mutta se on toistaiseksi osoittautunut hämmästyttävän kestäväksi kohteeksi.

Yksilöiden ja organisaatioiden kohdalla merkittäviin psykologisiin vaikutuksiin varautumisen tulisi kuitenkin muodostua normiksi. Niiltä puuttuu yleensä yhteiskuntien kaltainen kriisinkestävyys, joten psykologiset seuraukset voivat olla paljon vakavampia. Kyberhyökkäyksen aiheuttaman kriisin keskellä organisaatioiden olisi kiinnitettävä nykyistä enemmän huomiota työntekijöidensä henkiseen hyvinvointiin. Tilanne voi olla vakava, ja vahinkojen rajoittaminen vaatii usein kaikilta tavallista suurempia ponnituksia, mutta liian kova paine ja liian pitkät päivät voivat lopulta vahingoittaa työntekijöitä itseään. Suomen turvallisuusstrategiassa yhdeksi elintärkeäksi toiminnoksi on määritelty henkinen kriisinkestävyys. Jatkossa sen merkitys entisestään korostuu ja kyberpsykologinen vaikuttaminen tulee ottaa entistä paremmin huomioon.



LÄHTEET:

<https://databreachclassaction.io/blog/the-psychological-impact-of-data-breaches-on-victims>
<https://journals.sagepub.com/doi/10.1177/13691481231210383>
<https://www.tandfonline.com/doi/full/10.1080/19331681.2024.2420669#abstract>
<https://academic.oup.com/jogss/article/8/1/ogac042/6988925?login=false>
<https://www.bleepingcomputer.com/news/security/from-cipher-to-fear-the-psychology-behind-modern-ransomware-extortion/>
<https://puolustusvoimat.fi/documents/1951253/2815786/2025-3%20Psychological%20effects%20of%20cyberattacks.pdf/9d278114-e577-7359-2c9b-40750b6976be?t=1741783617259>
<https://www.techradar.com/pro/the-aftermath-of-the-kyivstar-cyber-attack-is-a-warning-for-us-all>
<https://besacenter.org/the-cyber-domain-in-the-russo-ukrainian-war/>
<https://besacenter.org/the-cyber-domain-in-the-russo-ukrainian-war/>
<https://www.esecurityplanet.com/threats/the-shadow-war-predatory-sparrow-vs-irans-infrastructure/>
<https://www.usnews.com/news/politics/articles/2026-03-29/hacked-hospitals-hidden-spyware-iran-conflict-shows-how-digital-fight-is-ingrained-in-warfare>
<https://www.csis.org/analysis/how-will-cyber-warfare-shape-us-israel-conflict-iran>
<https://zendata.security/2026/03/02/cyber-warfare-in-the-us-israel-vs-iran-conflict-roaring-lion-epic-fury/>
<https://www.rusi.org/explore-our-research/publications/commentary/fog-proxies-and-uncertainty-cyber-us-israeli-operations-iran>
<https://raaznet.com/en/reports/inside-irans-national-information-network>
<https://www.chathamhouse.org/2026/01/irans-internet-shutdown-signals-new-stage-digital-isolation>
<https://bit.sbu.ac.ir/Lab/ByFaculty>
https://ds.sndu.ac.ir/article_562.html
<https://civilica.com/doc/633994>
<https://civilica.com/doc/539792>
https://ds.sndu.ac.ir/article_562.html
<https://yle.fi/a/3-12152682>



Palvelut

Cyberwatch Finland on kyberjohtamisen ja strategisen kyberturvallisuuden luotettava sekä osaava kumppani ja palvelun tuottaja.

Kyberturvallisuuskapasiteetin rakentaminen

Cyberwatch Finland on strategiseen kyberturvallisuuteen erikoistunut konsulttiyritys, joka palvelee yrityksiä ja muita organisaatioita kehittämällä niiden kykyä ennakoimaan ja estämään kyberhyökkäyksiä. Yritys perustettu helmikuussa 2017. Cyberwatch Finland liittyi osaksi Netum Groupia 21.4.2026. Autamme yrityksiä ja organisaatioita joustavilla ratkaisuilla, laadukkailla palveluilla ja laajalla tietopohjalla.

Cyberwatch Finland palvelee yrityksiä ja muita organisaatioita vahvistamalla ja kehittämällä niiden kyberturvallisuuskulttuuria. Tavoitteenamme on strategisen kybertietoisuuden ja -kyvykkyyden parantaminen toiminnan kaikilla tasoilla, yksittäisistä henkilöistä organisaatioiden ylimpään johtoon asti. Tiedotamme tämän hetken kyberturvallisuusilmiöistä ja niihin vaikuttavista tekijöistä.

Palvelumme



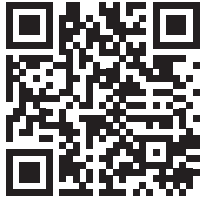
- Verkkoanalyysi (darkSOC®) ja Toimitusketjujen turvallisuus
- Tilannekuvapalvelu (Viikko- ja kuukausikatsaukset)
- Teema- ja erikoisraportit (tilauksesta)
- Koulutus ja osaamisen kehittäminen: (Cyberwatch- koulutusmoduulit ja luennot, Henkilöstön kybertilante-tietoisuus, Organisaatiokohtainen & roolipohjainen koulutuspaketti)
- Johdon neuvontapalvelut (mm. erilaiset skenaario- ja kriisinhallintatyöpajat) ja Cyber Due Diligence
- Tekoälyavusteinen kyberriskien hallintamalli
- NIS2 Yrityskonsultaatio

Luomme lisäarvoa:

- 1 Dark web- ja deep web -palveluillamme olemme edelläkävijöitä organisaatioiden ennaltaehkäisykyvyn rakentamisessa.
- 2 Tuotamme organisaatiokoh-taista, ajantasaista tilannekuvaa ja uhkatiedustelutietoa – tiedä uhat ennen kuin ne iskevät.
- 3 Rakennamme älykkäitä kyberturvallisuuspalveluita, ja painopisteemme on ketterissä ja vaikuttavissa kyberriskien hallintaprosesseissa.

Cyberwatch Finlandin kyberturvallisuuden palvelut

– kaikkiin yrityksen elinkaaren vaiheisiin



1. LÄHTÖTILANTEEN KARTOITUS

- Tarkastetaan yrityksen kybermatu-riteetti käyttäen esim. kyberturval-lisuuden nykytila-analyysiä
- Verkkoanalyysi ja haavoittuvuus-pinta-alakartoitus & Toimintaympä-ristöanalyysi

2. TOIMINNAN VAKIINNUT-TAMINEN JA KOULUTUS

- Koulutus
- Kyberturvallisuusregulaatio & ohjeistus
- NIS2-yrityskonsultaatio
- Kyberturvallisuuden kehittämis-suunnitelma

3. TILANNEKUVAN YLLÄPITO

- Johdolle ja henkilöstölle
- Tilannekuvapalvelu: viikko- ja kuukausikatsaus

4. KYBERRISKIEN HALLINNAN KEHITTÄMINEN JA YLLÄPITO & KYBERTILANTEEN JATKO-SEURANTA

- Kyberriskien hallintasuunnitelma
- Ylläpidetään tilannekuvaa (esim. verkkoanalyysin jatkuva seuranta)
- Lisäkoulutuksen tuottaminen

5. KEHITYKSEN TUKENA

- Toimitusketjun auditointi
- Taustaselvitykset
- Cyber Due Diligence
- Kyberriskipohjainen päätöksente-ko (skenaariot)

6. JATKUVUUDENHALLINTA

- Johdon neuvontapalvelut
- Kyberriskien hallintatoimen-piteidenseuranta ja kehittäminen
- Kriisijohtamisharjoitus

Organisaatioiden haasteet

- ! nopeasti muuttuvat kyberuhat
- ! rajallinen näkyvyys riskeihin
- ! kasvavat sääntelyvaatimukset (NIS2)
- ! toimitusketjujen kyberriskit

Ratkaisumme

- ✓ Kyberuhkien tilannekuvapalvelu
- ✓ Strateginen analyysi ja Kyberuhkatiedustelu
- ✓ Helppokäyttöinen kyberriskien hallintamalli
- ✓ Pimeän ja syvänverkon analyysi (darkSOC)

Kyberturvallisuus jää usein IT-tasolle, vaikka sen tulisi olla strategisen riskienhallinnan osa.



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

CYBER SECURITY NORDIC

28–29 Oct 2026

Helsinki Expo and Convention Centre

/MESSUKESKUS



Ron Deibert

Founder and Director,
Citizen Lab,
University of Toronto



Susann Lüdtkke

CEO & Founder,
L.I.A. – Lüdtkke Intelligence
& Analytics



Paolo Palumbo

VP, Strategic Threat
Intelligence & Research,
WithSecure™



Holger Haljand

CEO,
Telia Finland Oyj



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