# Cyberwatch Finland

## WHITEPAPER 2025

# KRIITTISTEN KOMMUNIKAATIO-JÄRJESTELMIEN TULEVAISUUDEN HAASTEET JA RATKAISUT

Kyberturvallisuus syntyy pienistä teoista ja kokonaisuuden hallinnasta

# SISÄLTÖ
















**Cyberwatch** WHITEPAPER

| | |
|---|---|
| JULKAISIJA | Cyberwatch Oy<br>Nuijamiestentie 5 C<br>Helsinki, Finland |
| SISÄLTÖ | Toimitusjohtaja<br>Aapo Cederberg<br>aapo@cyberwatchfinland.fi |
| TAITTO | PuulaMedia / Mari Riepponen |
| KUVAT | AdobeStock |
| PAINO | Scanseri Oy, Helsinki |
| ISSN | 2490-0753 (print) |
| ISSN | 2490-0761 (web) |

# Johdanto

**Teknologia kehittyy** nopeammin kuin koskaan ennen, ja sodat Ukrainassa ja muualla maailmassa korostavat karulla tavalla haasteita, joita kriittinen infrastruktuuri kohtaa näin vaikeissa olosuhteissa. Etenkin EU-alueella niihin pyritään vastaamaan uudella sääntelyllä, mutta usein se myös saa samalla aikaan uusia haasteita. Eräs kriittisen infrastruktuurin keskeinen osa ovat kriittiset kommunikaatiojärjestelmät, joiden tulevaisuus nyky-yhteiskunnissa on hyvin monisäikeinen ja siten hankalasti hallittavissa. Tämän haasteen tutkiminen ja siihen vastaaminen on tämän tutkimuspaperin tavoite. Eri puolilla maailmaa vallitsevista konflikteista on mahdollista ammentaa oppeja, ja niiden pohjalta voidaan kehittää tulevaisuuden ratkaisuja uutta teknologiaa hyödyntäen.

Data on keskeinen elementti niin yrityksissä kuin yhteiskunnan kriittisissä palveluissakin. EU:n datastrategian mukaan mahdollisuus datan laajaan saatavuuteen ja hyödyntämiseen on keskeinen edellytys innovaatioille ja kasvulle. EU:n tavoitteena on turvallinen ja dynaaminen datatalous, jossa datan kerääminen ja hyödyntäminen ovat keskeinen osa organisaatioiden toimintaa. Suurin osa globaalista arvonlisästä tehdään juuri digi- ja teknologiainnovaatioilla. Datan hyödyntäminen tarjoaa mahdollisuuksia arvonluontiin ja tuottavuuden kasvuun kaikilla talouden sektoreilla.

**Datatalous ja datakeskukset** liittyvät kiinteästi toisiinsa. Datakeskukset ovat välttämättömiä datatalouden toiminnan mahdollistamiseksi, sillä ne tarjoavat infrastruktuurin datan tallentamiseen ja käsittelyyn. Datatalouden merkitystä korostaa se, että pääministeri Orpon hallitus teetättää datatalouden tiekarttaselvityksen ajalla 18.6–31.10.2025. Hallituksen tavoitteena on toteuttaa datataloudesta laaja-alainen, strateginen teemakokonaisuus, jonka kärkiä ovat kvanttilaskenta, nopeat langattomat verkot, terveysdata, kyberturvallisuus, tekoäly sekä datatalouden edistäminen ja datan saatavuus tekoälyn käyttöön. Tässä kokonaisuudessa turvallisella kommunikaatioinfrastruktuurilla on keskeinen merkitys.

**Datan hyödyntäminen tarjoaa mahdollisuuksia arvonluontiin ja tuottavuuden kasvuun kaikilla talouden sektoreilla.**

Kolmas keskeinen muutosajuri on tekoälyn käyttö verkostotoiminnassa. Tekoälyn avulla voidaan ulkoistaa ihmisten ymmärrystä. Tekoälyn ja datan avulla voidaan käyttäjille kehittää älykkäitä neuvonantajia, opettajia tai avustajia, jotka voivat auttaa monimutkaisissa päätöksentekotilanteissa. Jo nyt generatiivisesta tekoälystä on tullut laajasti käytetty tuki teollisuudessa, julkishallinnossa ja ihmisten arjessa. Tekoäly ja koneoppiminen ovat myös tulleet sekä kyberhyökkääjien että -puolustajien käyttöön. Käynnissä olevassa datan ja tietoliikenteen transformaatiossa pyritään rakentamaan tekoälyä hyödyntävä data- ja verkkokeskeinen toimintakonsepti, jolla voidaan tehostaa päätöksentekoa toiminnan eri tasoilla sekä sotilas- että siviilitoimintaympäristössä.

# 1 Regulaatio ohjaa kehittämistä

**Tulevaisuuden tuotteiden** vaatimuksia pohdittaessa on parasta aloittaa tarkastelemalla, mitä vaatimukset ovat juuri nyt. Looginen ensimmäinen askel on tarkistaa lainsäädäntö, tässä tapauksessa NIS2-direktiivi ja sen myötä Suomessa säädetty tuore laki kyberturvallisuudesta. Viestintäteknologiaa koskevia olennaisimpia vaatimuksia ovat viestintäverkkojen ja -järjestelmien suojaaminen, järjestelmien erottaminen ulkopuolisista ympäristöistä, kulunvalvonta sekä säännölliset päivitykset. Lisäksi järjestelmien on oltava käyttökelpoisia myös vakavien häiriöiden ja poikkeusolojen aikana. Tämä edellyttää sekä digitaalista että fyysistä resilienssiä.

Järjestelmien häiriökestävyyden eli resilienssin merkittävimmät tekijät ovat ajantasaiset varmuuskopiot sekä käyttökelpoiset ja toimivat varajärjestelmät. Häirittyjen tai muutoin rikottujen järjestelmien korjaamisen on myös tapahduttava mahdollisimman ripeästi. Kaksikäyttöjärjestelmät ovat yksi tapa keventää tätä taakkaa, koska siviili- ja sotilasjärjestelmien välillä vaihdettavat komponentit ja henkilöstö voivat nopeuttaa huomattavasti järjestelmien korjaamista. Se mahdollistaa myös sotilaallisten järjestelmien skaalaamisen kriisitilanteiden aikana nopeammin kuin muuten olisi mahdollista. Kaksikäyttötuotteet eivät ole ongelmattomia, ja etenkin erilaiset turvallisuusvaatimukset perinteisten siviili- ja sotilaskäyttötapausten välillä tuottavat haasteita. Tällaisten tuotteiden kehittäminen tarjoaa silti kilpailuetua yrityksille, jotka haluavat menestyä nykyisessä geopoliittisessa ympäristössä.

**On kuitenkin pidettävä** mielessä riskiperusteinen lähestymistapa kaksikäyttötuotteisiin. Sitä vaaditaan kyberlainsäädännössä ja kriittisten toimijoiden häiriönsietokykyä koskevassa direktiivissä, ja se on myös avain sotilaallisten käyttötapausten turvallisuusvaatimusten ymmärtämiseen. Kaikkea dataa ei esimerkiksi kannata käsitellä samalla laitteella, koska järjestelmään tunkeutunut hyökkääjä saisi tällöin kaiken välittömästi haltuunsa. Järjestelmän turvallisuus on vain niin vahva kuin sen heikoin lenkki, joten tiedon lokeroiminen ja pääsyn rajaaminen ovat välttämättömiä toimia turvallisuuden takaamiseksi. Tämä pätee myös kriittiseen infrastruktuuriin, ja järjestelmien erottaminen toisistaan voi olla tehokas tapa estää yksittäisiä uhkia lamauttamasta kokonaisia valmiuksia.

Regulaatioprosessin seuraava vaihe liittyy Euroopan parlamentin ja neuvoston asetukseen koskien digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksia. Tämän kyberkestävyyssäädöksen pohjalta annetaan kansallinen toimeenpanolaki vuoden 2025 aikana. Kyberkestävyyssäädöksen taustalla on kyberturvallisuuteen liittyvä kehitys, jossa laitteet ja ohjelmistot joutuvat enenevässä määrin kyberhyökkäysten kohteeksi. Kyberkestävyyssäädöksen yleisenä tavoitteena on luoda olosuhteet turvallisten digitaalisen elementin sisältävien tuotteiden kehittämiselle ja varmistaa, että laitteissa ja ohjelmistoissa on vähemmän haavoittuvuuksia ja valmistajat ottavat turvallisuusnäkökohdat vakavasti huomioon tuotteen elinkaaren ajan.

**Toisena tavoitteena on** lisätä laitteiden käyttäjille näkyvyyttä tuotteiden kyberturvallisuusominaisuuksiin. Kyberkestävyysasetus on asetuksena suoraan sovellettava, eikä se lähtökohtaisesti sisällä kansallista liikkumavaraa. Kansallisesti voidaan asettaa vaatimuksia kyberturvallisuuden sertifiointijärjestelmien käytölle ja määritellä viranomaisen valvonta- ja ilmoitusvastuut. Säädös ja toimeenpanolaki luovat alan toimijoille merkittäviä toimenpidevaatimuksia.

**Järjestelmän turvallisuus on vain niin vahva kuin sen heikoin lenkki, joten tiedon lokeroiminen ja pääsyn rajaaminen ovat välttämättömiä toimia turvallisuuden takaamiseksi.**

# 2 Tärkeimmät opit Ukrainan sodasta ja viimeaikaisista kyberoperaatioista

**Ukrainan sota** on osoittanut, kuinka monipuolisia modernin sodankäynnin menetelmät ovat ja kuinka nopeasti ne voivat kehittyä. Sodan alussa Venäjä hyökkäsi ikään kuin umpimähkään kaikkiin löytämiinsä kohteisiin, mutta sen jälkeen hyökkäykset kyberavaruudessa ovat muuttuneet täsmällisemmiksi ja kohdennetummiksi. Nykyään painotetaan enemmän tiedustelutietojen keräämistä ja hyökkäysten räätälöintiä kullekin kohteelle parhaiden mahdollisten tulosten saavuttamiseksi. Ne ovat myös aiempaa tiiviimmin sidoksissa muihin sotilas- ja informaatio-operaatioihin.

Ukraina oli jo parantanut kybervalmiuksiaan vuoden 2022 täysimittaista hyökkäystä edeltävinä vuosina esimerkiksi ottamalla käyttöön automatisoituja prosessinohjausjärjestelmiä ja niihin liittyviä kyberturvallisuusmekanismeja. Nämä järjestelmät ovat onnistuneesti tarjonneet korkeatasoisen suojan ja toimivuuden sodanajan olosuhteissa. Lisäksi Ukrainan suurimmat operaattorit sopivat välittömästi kansallisten verkkovierailuiden sallimisesta palveluiden takaamiseksi ja langattomilla tukiasemilla sekä moderneilla teknologisilla ratkaisuilla pystyttiin rakentamaan yhteydet suojatiloihin ja muihin maanalaisiin verkkoihin.

**Ukrainalaisten lähteiden** mukaan toinen onnistuneen kyberpuolustuksen keskeinen lähtökohta on, kenties hieman ironisesti, hyökkäävien kybervalmiuksien tehokas käyttö. Näyttää siltä, että hyökkäys on paras puolustus myös kyberavaruudessa. Keskeisiä ajatuksia tämän näkökul-

man taustalla ovat pelote, ennaltaehkäisevät iskut sekä tehokkaat vastatoimet. Aktiivisessa sotatilassa pelote jää taka-alalle, mutta erityisesti ennaltaehkäisevät iskut korostuvat, koska vihollisen kyvykkyyksien lamauttaminen tai tuhoaminen ennen kuin se ehtii toteuttaa onnistuneita hyökkäyksiä on kenties kaikkein tehokkain puolustusmuoto.

Venäjän kyberhyökkäyksille haavoittuvimmat kohteet ovat olleet Ukrainan kriittisen infrastruktuurin osat. Hyökkäyksiä on tehty jo yli vuosikymmenen ajan, ja uusia toteutetaan jatkuvasti. Tehokkaimmat operaatiot ovat johtaneet esimerkiksi laajoihin sähkökatkoihin, viestintäverkkojen täydelliseen sulkemiseen ja kasvavaan yleiseen epäluottamukseen sekä valtion laitoksia että yksityisiä yrityksiä kohtaan. Tämä korostaa siviili-infrastruktuurin resilienssin valtavaa merkitystä. Vaikka kaikki kyberalan hyökkäykset eivät kohdistu siviileihin, ne tarjoavat usein helpompia kohteita kevyempien turvatoimien ansiosta. Venäjä on viime aikoina siirtänyt huomionsa kaikkeen, mikä liittyy edes epäsuorasti sotatoimialueeseen, mukaan lukien hyökkäyksiin palveluntarjoajia vastaan. Niiden tarkoituksena on tunkeutua sodankäyntiin ja politiikkaan liittyviin järjestelmiin huomaamatta ja ylläpitää niissä läsnäoloa. Hakkerit eivät enää hyödynnä vain satunnaisia haavoittuvuuksia, vaan kohdistavat iskunsa nyt tarkoituksellisesti kohteisiin, jotka ovat kriittisiä sotilasoperaatioiden onnistumisen ja tukemisen kannalta.

**Hakkeroinnin menestys** kaupallisella sektorilla selittyy myös sillä, että Ukrainan asevoimat mukauttavat ja ottavat kaupallisia teknologioita yhä enemmän sotilaskäyttöön. Se tekee tällaisiin teknologioihin kohdistuvista ennaltaehkäisevistä kyberoperaatioista strategisesti lupaavan hyökkäysvektorin lähitulevaisuudessa. Ukraina käsitteli kolme miljoonaa tietoturvapoikkeamaa vuonna 2024. Näistä yli 4 315 tapausta vahvistettiin selkeiksi kyberoperaatioiksi. Kasvua edellisestä vuodesta oli lähes 70 %.

Standardoidun laitteiston ja infrastruktuurin käyttöönotto organisaatioissa parantaa merkittävästi häiriönsietokykyä ja helpottaa nopeaa toipumista kyberhäiriöiden jälkeen. Yksityisen sektorin, vapaaehtoisten ja erityisesti kumppanivaltioiden yhteistyön ja tuen merkitys on korostunut koko Ukrainan sodan ajan. Venäjä vihollisena ymmärtää vain voimaa ja ainoa tapa vaikuttaa sen toimiin on projisoida voimaa eri kanavien kautta. Kyberulottuvuus on yksi näistä, ja voiman projisointi siellä on välttämätöntä sekä Ukrainalle että kaikille Venäjän hyökkäysoperaatioiden kohteena oleville maille. Sodan vuoksi Venäjä ja Ukraina kehittyvät kybersodankäynnissä noin 10 kertaa nopeammin kuin sodan ulkopuoliset valtiot, joten niiden konfliktin kehityksen seuraaminen on välttämätöntä nykyisten kybervalmiuksien ja -trendien ymmärtämiseksi.

**Standardoidun laitteiston ja infrastruktuurin käyttöönotto organisaatioissa parantaa merkittävästi häiriönsietokykyä ja helpottaa nopeaa toipumista kyberhäiriöiden jälkeen.**

**Kyberoperaatiot ovat olleet** läsnä myös muissa viimeaikaisissa konflikteissa. Pakistan ja Intia käyttivät kyberhyökkäyksiä täydentääkseen muita operaatioita kevään lyhyen yhteenoton aikana, ja Israel ja Iran tekivät samoin kesäkuussa. Konfliktin aikana Pakistan oli erittäin aktiivinen hyökkäyksellisissä kyberoperaatioissa, ja joidenkin lähteiden mukaan intialaisia kohteita vastaan tehtiin yli 1,5 miljoonaa hyökkäystä. Pakistan julisti, että heidän hyökkäyksensä olivat valtava menestys, ja niiden tuloksiin kuului väitetysti esimerkiksi 70 prosenttia Intiasta kattanut sähkökatkos. Villeimmät väitteet ovat myöhemmin osoittautuneet vääriksi, mutta Pakistan hyödynsi niitä menestyksekkäästi informaatio-operaatioissaan ennen sitä. Selkeä rinnastus voidaan vetää siihen, miten Venäjä sitoo informaatio- ja kyberoperaationsa yhteen. Suurin osa onnistuneista operaatioista oli vain yksinkertaisia palvelunestohyökkäyksiä, jotka kohdistuivat valtion ja yksityisen sektorin verkkosivustoihin Intiassa. Intian kostotoimet olivat hyvin pieniä, mikä saattaa viitata siihen, että maalla ei ole kybervalmiuksia, jotka voisivat kilpailla suoraan Pakistanin kanssa.

Iranin ja Israelin välinen konflikti oli erilainen. Molemmat maat ovat investoineet kybervalmiuksiin jo vuosia tai jopa vuosikymmeniä, ja molempia tukevat myös erilaiset kansalaisjärjestöt ja poliittisesti motivoituneet haktivistit. Kyberhyökkäysten määrä Israelissa kasvoi lähes kymmenkertaiseksi sen jälkeen, kun se aloitti ilmaiskut Iranissa. Suurin osa hyökkäyksistä oli jälleen suhteellisen harmittomia palvelunestohyökkäyksiä tai verkkosivustojen turmelemisia. Mielenkiintoinen seikka hyökkäyksissä on se, kuka niitä tekee. Suurin osa hyökkäyksistä tulee kolmansilta osapuolilta, kuten palestiinalaismielisiltä ryhmiltä tai islamistihakkereilta

On hyvin vaikeaa saada minkäänlaista tarkkaa tietoa Iraniin kohdistuneista hyökkäyksistä, koska maa käytännössä sulki itsensä internetistä melko varhain konfliktin alussa. Kyseessä on mielenkiintoinen strategia hyökkäysten välttämiseksi, mutta toistaiseksi sen tehokkuutta on vaikea arvioida. Ennen internetin sulkemista tapahtui kuitenkin tiettävästi ainakin yksi merkittävä isku. Sen seurauksena israelilainen ryhmä onnistui sulkemaan suurimman osan Iranin pankkisiirroista. Häiriöiden todellista laajuutta on vaikea selvittää, mutta monet ira-

nilaiset tiedotusvälineet raportoivat laajoista pankkihäiriöistä ja kansalaisten vaikeuksista päästä tileilleen tai nostaa rahaa.

**Sodassa ja konflikteissa** korostuu tiedustelun osuus. Esimerkiksi Ukrainalle tiedustelutiedot ovat yhtä keskeisiä kuin sen saama aseapu. Strategisen tiedustelun avulla Ukraina saa kuvan Venäjän strategisen tason tavoitteista. Operatiivisella ja taktisella tasolla voidaan tiedustelutiedon avulla ohjata eri puolustushaarojen operaatioita kyberoperaatiot mukaan lukien. Suorituskyky tiedusteluympäristössä edellyttää kommunikaatiosektorin hallintaa. Taistelukentällä on erittäin paljon toimijoita ja järjestelmiä. Taistelijat, asejärjestelmät, miehitetyt ja miehittämättömät ilma-, maa- ja merialukset sekä kommunikaatiolaitteet muodostavat dynaamisen ja verkottuneen kokonaisuuden.

Yhdysvalloissa on huomattu kommunikaation ja datan yhteistoiminnan merkitys. Yhdysvaltain puolustusministeriön Combined Joint All-Domain Command and Control (CJADC2) -konseptin tarkoituksena on yhdistää kaikki taistelukentän eri resurssit (ilma, maa, meri, avaruus ja kyber) yhdeksi datakeskeiseksi, integroiduksi ja tekoälytuetuksi verkostokokonaisuudeksi. Konseptin tavoitteena on parantaa tilannekuvaa taistelukentällä, nopeuttaa ja tarkentaa päätöksentekoa sekä tehostaa sotilasoperaatioita mahdollistamalla saumaton tiedonjakaminen ja kommunikaatio puolustushaarojen eri toimijoiden välillä. Tämä mahdollistaa tiedon saannin missä ja milloin tahansa nopeita päätöksiä varten. Konsepti käsittää myös kumppaneiden ja liittolaisten liittämisen osaksi kokonaisuutta.

**Suorituskyky tiedusteluympäristössä edellyttää kommunikaatiosektorin hallintaa.**

**Kyberulottuvuudella näyttää olevan** tukeva rooli kineettisissä konflikteissa maailmanlaajuisesti, mutta se toimii myös hybridisodankäynnin välineenä. Viime aikoina se on ollut ennen kaikkea keskeinen osa informaatio-operaatioita. Venäjän osalta näyttää siltä, että suurin osa kyberresursseista kohdistuu Ukrainaa tukeviin maihin, ei Ukrainaan itseensä. Tämä selittyy kyvyllä iskeä Ukrainaan kineettisin keinoin, sillä sitä Venäjä ei voi tehdä muihin lännessä sijaitseviin kohteisiin. Toisaalta erilaiset sabotaasioperaatiot ja esimerkiksi tietoliikennekaapeleiden vaurioittaminen Itämerellä voidaan nähdä tietynlaisena kineettisenä vaikuttamisena. Aivan kuten Ukrainassa, kommunikaatiojärjestelmät näyttävät olevan Venäjän operaatioiden ensisijainen kohde myös Ukrainaa tukevissa maissa. Kyberhyökkäyksillä tulee edelleen olemaan merkittävä rooli hybridivaikuttamisessa. Vaikka Ukrainaan saataisiin tulitauko, se ei lopettaisi Venäjän kyberoperaatioita, joita se pyrkii jatkamaan sodankäynnin kynnyksen alapuolella. Tämän vuoksi kansallista resilienssiä on vahvistettava edelleen.

# 3 Informaatio-operaatiot tukevat kyberhyökkäyksiä

**Siviiliyhteiskunta on houkutteleva** kohde informaatio-operaatioille, ja Venäjä on liittänyt ne yhä useammin kyberhyökkäyksiin, mikä näkyy myös siinä, mitkä operaatiot ovat olleet kaikkein onnistuneimpia. Venäjän informaatio-operaatiot Ukrainan ulkopuolella ovat niin ikään kohdistuneet siviiliyhteiskuntiin pyrkimyksenä muuttaa yleistä mielipidettä kohti narratiiveja, joita Venäjä voisi paremmin hyödyntää. Niihin sisältyy sekaantuminen demokraattisiin vaaleihin ja poliittiseen päätöksentekoon lännessä, ja jotkut jopa sanovat, että Venäjä harjoittaa ”vaaleihin sekaantumista palveluna”. Tämä tarkoittaa sitä, että tietyt poliitikot ottavat yhteyttä venäläisiin pyytääkseen heiltä tukea informaatio-operaatioiden muodossa. Operaatioiden tarkoituksena on auttaa kyseisiä ehdokkaita tulemaan valituiksi.

Venäjä hyödyntää laajasti tekoälyä informaatiotoiminnassaan tuottaakseen loputtomasti sisältöä sosiaaliseen mediaan ja muille vastaaville alustoille. Vain hieman yli kaksi vuotta tekoälyn suurten kielimallien julkistamisen jälkeen on havaittu tapauksia, joissa pahantahtoiset toimijat ovat käyttäneet generatiivista tekoälyä haitallisten ja väärien narratiivien massatuotantoon. Nyt Venäjän ilmeinen yritys on saastuttaa tekoälychatbotteja tuottamallaan propagandalla. Venäjä käyttää tekoälyä informaatiotoiminnassaan tuottaakseen loputtomasti sisältöä sosiaaliseen mediaan ja muille vastaaville alustoille. Nämä alustat levittävät valheita ohjeistamalla tekoälymalleja massatuottamaan vääriä narratiiveja. Niillä esimerkiksi luodaan tuhansia disinformaatiota sisältäviä artikkeleita ja julkaistaan ne verkossa.

**Internetin saastuttamiseen** käytettävä Prompt infection -hyökkäys kohdistuu laajoihin kielimalleihin (Large language models, LLM) lisäämällä haitallista tai harhaanjohtavaa tekstiä syötteisiin, jolloin LLM tuottaa tahattomia tai haitallisia tuloksia. Tällä menetelmällä manipuloidaan ja vääristetään LLM:n toimintaa. Synteettinen tietosisältö (esim. deepfake-videot) lisääntyy nopeasti eri media-alustoilla. Ne voivat sisältää erityyppistä sisältöä, kuten kuvia, videoita, ääntä ja tekstiä. Synteettisen sisällön luomiseen käytetty teknologia koulutetaan usein olemassa olevan, todellisen verkosta löytyvän sisällön pohjalta. Tämä tarkoittaa, että synteettinen tietosisältö näyttää realistiselta ja sitä on hyvin vaikea erottaa aidosta mediasisällöstä. Synteettinen tietosisältö pahantahtoisten toimijoiden käsissä vaikuttaa merkittävästi informaatioturvallisuuteemme.

Venäjä-taustainen Pravda-verkosto on toimija Venäjän hybridisodankäynnin maailmassa. Verkosto koostuu 182 uniikista internet-verkkotunnuksesta ja aliverkkotunnuksesta, jotka kohdistuvat vähintään 74 maahan ja alueeseen sekä 12 yleisesti puhuttuun kieleen. Sen arvioidaan tuottavan yli 3,6 miljoonaa Venäjää tukevaa disinformaatioartikkelia vuosittain. Tuloksena hakukoneet ja LLM-pohjaiset tekoälyt (esim. ChatGPT) toistavat siten Venäjän propagandaa.

**Venäjä käyttää tekoälyä** myös tiedusteluun ja haavoittuvuuksien hyödyntämiseen kyberoperaatioissa. Tekoälyn käytöstä ja muusta teknologian kehityksestä huolimatta ihminen on edelleen heikoin lenkki kyberturvallisuuden ja haavoittuvuuksien hallinnan ketjussa. Henkilöstön kybertietoisuuden lisääminen ja kyberhygienian korkean tason ylläpitäminen ovat edelleen keskiössä. Tietojenkalasteluhyökkäykset, haittaohjelmien käyttöönotto ja bottiverkkojen luominen ovat Venäjän tällä hetkellä tietovarkauksiin ja tieto- ja viestintäjärjestelmien häirintään suosimia keinoja. Hakkerit kohdistavat toimintaansa yhä useammin pikaviestintileihin levittääkseen haittaohjelmia ja käynnistääkseen tietojenkalastelukampanjoita, joiden tarkoituksena on vaarantaa mahdollisimman monet käyttäjät. Uhrin yhteystietojen joukossa voi olla arvokkaita kohteita, joiden viestihistoria kiinnostaa hyökkääjämaan tiedustelupalveluja.

# 4 Tulevaisuuden viestintäratkaisut strategisena kyvykkyytenä globaalissa kontekstissa

**Ukrainan sota** on opettanut paljon resilienssin merkityksestä ja siitä, miten nykyiset viestintäjärjestelmät toimivat sota-ajan ympäristössä. Mutta entä tulevaisuus? Jotta voisimme saavuttaa näkemyksen siitä, mitkä ovat kommunikaatiojärjestelmien vaatimukset ja mahdollisuudet tulevina vuosina, ei riitä, että tutkitaan vain menneitä tapahtumia tai nykyisiä ratkaisuja. Sen sijaan on mahdollista tehdä johtopäätöksiä tulevaisuuden viestinnän vaatimuksista selvittämällä, mitkä ovat ne haasteet, joihin ei vielä ole olemassa ratkaisuja ja minkälaisia mahdollisuuksia sekä haasteita uudet teknologiset innovaatiot voivat tuoda tullessaan.

## 4.1 Täydentäviä järjestelmiä tarvitaan

**Ensin on hyvä todeta,** että varajärjestelmien tarve ei katoa mihinkään. Konfliktitilanteessa, olipa se sitten kineettinen tai kyberluonteinen, hyökkäys onnistuu lopulta poistamaan käytöstä ainakin osan järjestelmästä. Kun näin tapahtuu, resilienssi eli järjestelmien häiriökestävyys astuu kuvaan. Se tarkoittaa, että ensisijaisen järjestelmän korjauksen tai korvauksen on oltava mahdollisimman helppoa ja nopeaa, ja sen aikana on oltava käytössä jonkinlainen varajärjestelmä, jotta toiminta voi jatkua ongelmista huolimatta. Yksi parhaista tavoista saavuttaa tämä on kaksikäyttöteknologioiden hyödyntäminen. Jos tuote soveltuu sekä sotilas- että siviilikäyttöön, on niitä yleensä enemmän, mikä puolestaan edesauttaa sitä, että logistiikkaketjut ovat tarpeeksi vahvoja. Se voi myös tarjota mahdollisuuden siirtää järjestelmän siviilikäytöstä sotilaskäyttöön tai päinvastoin, ja osia voidaan käyttää ristiin siviili- sekä sotilasjärjestelmien välillä. Käytännössä sotilaallisten järjestelmien skaalaaminen kriisitilanteiden aikana siis helpottuu. Riippumatta siitä, onko järjestelmä siviili- vai sotilaskäytössä, on tärkeää muistaa, että tehokas resilienssi edellyttää komponenttien lisäksi osaavan henkilöstön läsnäoloa järjestelmän lähellä, muuten korjauksia ei voida tehdä nopeasti.

Nopea militarisaatio ja kaupallisten teknologioiden integrointi sotilasoperaatioihin tuo mukanaan myös uusia turvallisuushaasteita. Monilta kaksikäyttöjärjestelmiltä, jotka on alun perin kehitetty siviilikäyttöön, puuttuu taisteluolosuhteiden edellyttämä häiriönsietokyky ja suoja. Erityisesti suojautuminen elektronisen sodankäynnin vaikutuksilta korostuu. Ennakoivien turvallisuusarviointien varmistaminen ja teknologioiden mukauttaminen sotilaallisiin tarpeisiin on olennaisen tärkeää. Jatkossa tähän olisi viisasta varautua jo kehitysprosessin aikana. Uudet tuotteet voidaan suunnitella kaksikäyttötapaukset huomioiden varsinkin silloin, kun on selvää, miten niitä käytetään molemmissa yhteyksissä.

**Ennakoivien turvallisuusarviointien varmistaminen ja teknologioiden mukauttaminen sotilaallisiin tarpeisiin on olennaisen tärkeää.**

**Vaihtoehtoisten järjestelmien käyttö** korostuu aktiivisilla sotatoimialueilla. Nykyisin Ukrainan rintamalle on muodostunut rintamalinjasta noin 40 kilometrin syvyinen vyöhyke, jossa sähkömagneettista spektriä hyödyntäviä laitteita ei juurikaan voi käyttää johtuen häirinnästä ja spoofingista. Lisäksi elekroninen tiedustelu paikantaa välittömästi radioiden, linkkien yms. lähettimien käytön. Siksi on kehitetty valokuituohjattuja drooneja, jolloin ei tarvitse käyttää radio- tai satelliittiyhteyksiä droonien ohjaamiseen. Tällä rintamalinjan alueella laitteiden lähetinosat pyritään sijoittamaan bunkkereihin. Lisäksi tarvitaan helposti käytettäviä valokuituyhteyksiä ja edullisia kenttäradioita taktisen tason kommunikaatioon. Tämä siksi, että radiot ovat nopeasti kuluvaa laitteistoa vahvan elektronisen sodankäynnin ympäristössä. Samalla Ukrainan sodankin perusteella on kuitenkin käynyt selväksi, että myös siviiliverkkoja käytetään tarvittaessa varajärjestelminä sotilaallisessa toiminnassa. Kustannustehokkaaksi varajärjestelmäksi viranomaistoimintaan voisi soveltua myös jokin tiedonsiirtonopeuksiltaan uutta Virve 2.0 -verkkoa vaatimattomampi radioverkko.

## 4.2 Järjestelmien on oltava muokattavia ja laaja-alaisia

**Järjestelmien tulee olla** muokattavia eri käyttötarkoituksiin ja -kohteisiin. Koska eri käyttäjillä on luonnollisesti erilaisia käyttötapauksia tuotteelle, sen mukauttamisen näihin tarpeisiin on oltava helppoa. Tämä on kaksikäyttötuotetta kehitettäessä pidettävä mielessä. Usein se voi merkitä sitä, että ensisijaisesti siviiliyhteiskunnan käyttämän järjestelmän turvallisuutta on parannettava, kun se siirretään sotilaskäyttöön. Esimerkiksi kriittisten palvelujen verkon viipalointi, joka takaisi ensisijaisen palvelun, pienemmän viiveen sekä nopeammat yhteydet, voi olla tärkeä ominaisuus monille potentiaalisille asiakkaille. Siinä asiakkaan verkkoliikenteelle raivataan ikään kuin yksityistie, jolloin muiden verkkoliikenne ei pääse vaikuttamaan verkon toimintaan. Nykyisten ennusteiden mukaan 5GSA otetaan laajalti käyttöön jo tänä vuonna. Viipalointia voitaisiin mahdollisesti käyttää myös turvallisuuden lisäämiseen esimerkiksi erottamalla armeijan käyttämä osa verkosta siviiliyhteiskunnan osuudesta.

Avoin radioverkko (Open Radio Access Network) on kehittyvä teknologia, jolla radioverkko voidaan optimoida avointen rajapintojen ja radioverkon toimintojen kehittyneen jaottelumallin avulla. Esimerkiksi osa tukiaseman toiminnoista voidaan siirtää pilvipalveluun siten, että se voi jakaa käytettävissä olevaa radiokapasiteettia tehokkaammin myös muille tukiasemille. Hyötynä on nykyistä parempi radioverkkojen

sisäisten rajapintojen yhteensopivuus eri toimijoiden kesken. Open-RAN-konsepti mahdollistaa myös kevyiden radioverkkojen nopean rakentamisen käyttäen hyväksi verkkotoimintojen prosessointia pilvipalveluissa ja COTS-komponentteja. Konseptista olisi hyötyä asevoimien operaatioissa dynaamisesti muuttuvissa taistelutilanteissa kentällä. Avoin radioverkkokonsepti tulee olemaan tärkeä mahdollisuus myös 6G-ympäristössä.

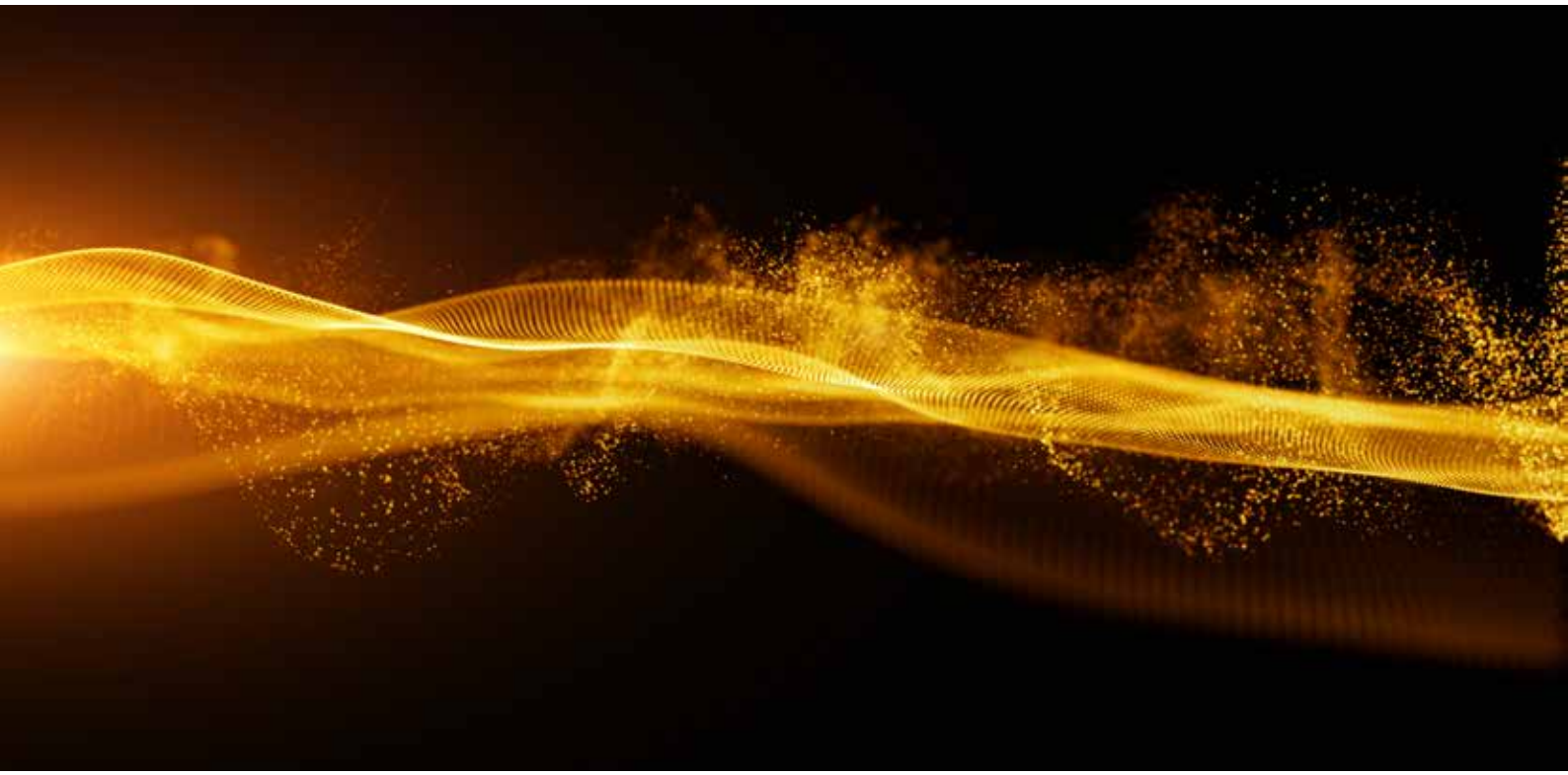
**Perinteiset RAN-arkkitehtuurit** tarjoavat hyvän perustan ja suorituskyvyn, jotka vastaavat pitkälti televiestinnän tarpeisiin. Liittämällä tekoäly RAN-arkkitehtuuriin voidaan lisätä järjestelmän tehokkuutta ja automaatiotasoa. AI-RAN:in avulla voidaan optimoida radioresurssien käyttöä ja taajuushallintaa sekä tehostaa mukautumista dynaamisesti muuttuviin tietoliikenne- ja taajuusolosuhteisiin parantaen näin järjestelmän kokonaistehokkuutta.

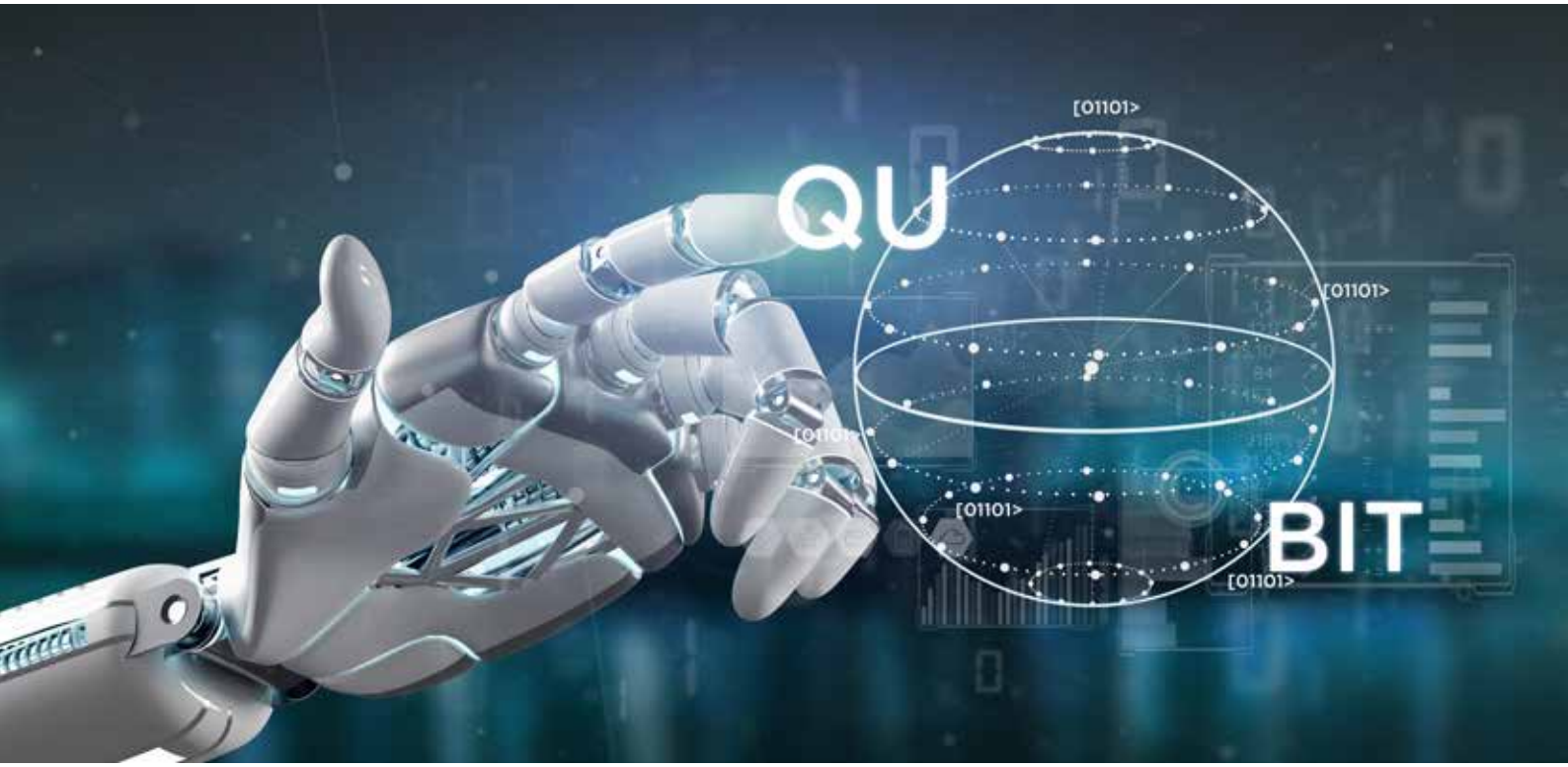
AI-RAN:in kehitys on sidoksissa reunalaskennan, pilvipalveluiden sekä tekoälyn kehittymiseen. AI-RAN-järjestelmän reaaliaikaiset toiminnot asettavat resurssi- ja viiverajoitusten vuoksi lisävaatimuksia tekoälyalgoritmien toteutukselle ja suorituskyvylle. Reunalaskenta voi auttaa tähän haasteeseen vastaamisessa. Sillä tarkoitetaan nimensä mukaisesti laskennan suorittamista ”reunalla”, eli pilven sijaan osa laskennasta tapahtuu fyysisesti lähellä päätelaitetta. Täten voidaan vähentää verkkoyhteyden ruuhkautumista sekä nopeuttaa vasteaikoja, kun pienempi määrä dataa on tarpeen siirtää paikasta toiseen. Reunalaskenta myös antaa kyberturvallisuudelle erilaisia mahdollisuuksia datan monipaikkaisuuden vuoksi.

Radiojärjestelmissä taajuusalueiden laaja käyttö lisää resilienssiä. Aikaisemmin kapeakaistaisena ja siirtokyvyltään rajoittuneena pidettyä HF-radiojärjestelmää kehitetään ohjelmistoradioteknologian avulla kohti kognitiivisuutta ja laajakaistaisuutta. Järjestelmässä käytetään sulautettua aaltomuodostusarkkitehtuuria, jossa kaikki tietoliikenteen osakomponentit on integroitu samaan aaltomuoto-ohjelmistoon. Aaltomuotoja kehittämällä voidaan parantaa HF-radioiden suorituskykyä ja tuottaa uusia toimintamahdollisuuksia.

**Mesh-järjestelmä on ryhmä** langattomasti toisiinsa yhteydessä olevia laitteita, jotka muodostavat yhtenäisen langattoman verkon. Mesh-radioverkossa useat radiot toimivat keskenään toistimina muodostaen verkoston, joka voi välittää suuria datamääriä pitkienkin matkojen päähän. Jokainen radio toimii sekä lähettimenä että vastaanottimena, ja ne käyttävät reititysprotokollaa siirtääkseen dataa parhaan reitin kautta. Mesh-verkot ovat joustavia ja skaalautuvia, ja ne tarjoavat redundanssia, mikä tarkoittaa, että jos yksi radio on toimintakyvytön, data voidaan silti siirtää toisen radion kautta. Mesh-radioverkot ovat hyödyllisiä kriittisissä viestintätilanteissa, joissa perinteiset viestintämuodot eivät toimi.

Taktisella tasolla voidaan rakentaa mobiiliverkkoratkaisuja, jotka tukevat valitulla alueella useiden satojen eri toimijoiden laitteiden ja asejärjestelmien päätelaitteita. Tällaiset paikalliset verkkoratkaisut tarjoavat käyttäjilleen kehittyneitä reunalaskentaominaisuuksia, mesh-verkkopalveluita, joustavaa taajuusalueiden hallintaa ja tehokasta kyberturvallisuutta. Paikallisista verkoista voidaan rakentaa hyvinkin joustavia ja nopeasti konfiguroitavia.






## 4.3. Järjestelmien on oltava luotettavia

**Keskeinen vaatimus** kommunikaatiojärjestelmille on luotettavuus. Ukrainan sotaa tarkasteltaessa viestiyhteyksien katkeaminen on ollut toistuva teema konfliktin aikana. Menetelmät, jotka kestävät paremmin häirintää ja muita häiriötilanteita, voisivat olla todella merkittäviä Ukrainan taistelukentillä ja tulevilla konfliktialueilla. Häirintä ei välttämättä edes edellytä aktiivista sotatilaa, kuten on havaittavissa esimerkiksi Etelä-Karjalassa, jossa Venäjä häiritsee matkapuhelinverkkoja ja GPS-signaaleja rajan läheisyydessä.

Tekoälyintegraatio voi osaltaan auttaa haasteisiin vastaamisessa. Tekoälypohjaiset ratkaisut voivat parantaa verkon tehokkuutta, vähentää viivettä ja mahdollistaa saumattoman yhteyden satelliitti-, ilma- ja maanpäällisissä verkoissa. Tekoäly voisi mahdollistaa monia ominaisuuksia, joita tarvitaan edellä mainittujen vaatimusten täyttämiseksi, olipa kyse sitten kaksikäyttöteknologioiden turvallisuuden parantamisesta tai älykkäistä menetelmistä signaalihäiriöiden välttämiseksi. Uusimpien standardien mukaiset verkkoarkkitehtuurit tukevat tekoälyn integrointia verkon laidoille lähelle niitä hyödyntäviä käyttäjiä, olivat ne sitten laitteita tai ihmisiä. On kuitenkin vielä selvittämättä, missä nämä ratkaisut tarkalleen ottaen toteutettaisiin ja kuka niitä hallitsisi, joten työtä riittää ennen käytännön harjoittelua ja toteutusta.

**Yksi merkittävimmistä** tekijöistä tekoälyn kehityksessä on kvanttilaskenta. Tämä johtuu siitä, että toisin kuin tavalliset tietokoneet, kvanttitietokoneet voivat tutkia kaikkia mahdollisia ratkaisuja samanaikaisesti superposition ja kvanttilomittumisen ansiosta. Kvanttitietokoneilla voidaan myös lyhentää tietoliikenteen salauksen purkamiseen tarvittavaa aikaa tuhansista vuosista jopa tunteihin tai minuutteihin. On ilmiselvää, että kvanttitietokoneiden kyvyllä murtaa melko helposti lähes kaikki tällä hetkellä käytössä olevat salausmenetelmät on valtava vaikutus kyberturvallisuuteen.

Huoltovarmuuskeskuksen mukaan organisaatioiden tulisi laatia suunnitelma kvanttikestäviin järjestelmiin päivittämiseksi siten, että kaikki kriittiset järjestelmät päivitetään vuoteen 2030 mennessä. Kenties paras mahdollinen tapa valmistautua tähän on etsiä "kryptoketteriä" järjestelmiä, eli sellaisia, joissa vaihtaminen salausmuodosta toiseen on helppoa. Tällä tavalla on paljon helpompaa pysyä ajan tasalla kvanttikestävien salausmenetelmien nopeassa kehityksessä. Kvanttilaskenta voi olla merkittävä myös positiivisilla tavoilla, sillä logistiikan optimoinnin kaltaiset asiat ovat sen avulla paljon helpompia kuin nyt. Vaikutus tekoälyyn tulee niin ikään olemaan valtava.

**Huoltovarmuuskeskuksen mukaan organisaatioiden tulisi laatia suunnitelma kvanttikestäviin järjestelmiin päivittämiseksi siten, että kaikki kriittiset järjestelmät päivitetään vuoteen 2030 mennessä.**

## 4.4 Tietoverkoissa tarvitaan joustavaa ja tehokasta tiedon suojausta

**Myös kyky jakaa tieto** eri suojausluokkiin, esimerkiksi julkiseen, luottamukselliseen ja salaiseen, on vaatimuksena tulevaisuuden kommunikaatiojärjestelmille. Ne voisivat helposti edustaa siviiliyhteiskunnan, kriittisen infrastruktuurin ja sotilasorganisaatioiden toimijoita sekä niiden kommunikaatioturvallisuutta koskevia vaatimuksia. Siviiliviestintää ei ehkä tarvitse suojata kvanttiuhkilta yhtä kiireisesti, kuin sotilaallista tai kriittisen infrastruktuurin viestintää, koska nämä kaksi ovat todennäköisemmin sellaisten vihamielisten toimijoiden kohteena, joilla on varhaisia kvanttivalmiuksia. Turvallisuusvaatimukset ovat muillakin tavoilla erilaiset, mikä on pidettävä mielessä kaksikäyttöjärjestelmiä suunniteltaessa.

On kuitenkin tärkeää muistaa, että toimivat kommunikaatiojärjestelmät ovat tärkeitä kaikille kolmelle ryhmälle. Vaikka asevoimat tarvitsevat niitä komentorakenteensa ylläpitoon sekä rauhan että sodan aikana, kuten kriittisen infrastruktuurin parissa työskentelevätkin, ei pidä unohtaa myöskään siviiliväestöä. Heille viestintäjärjestelmät mahdollistavat monia asioita virallisten tiedotteiden sekä uutisten saamisesta yhteydenpitoon läheisten kanssa. Viestintähäiriöt ovat osa kognitiivista sodankäyntiä, ja niillä on syvällinen vaikutus resilienssiin.

**Viestintähäiriöt ovat osa kognitiivista sodankäyntiä, ja niillä on syvällinen vaikutus resilienssiin.**

**Organisaatiotasolla (yritystasolla)** on ratkaisevan tärkeää toteuttaa vankka verkon segmentointi ja varmistaa sisäisten palvelujen, mukaan lukien kyberturvallisuusjärjestelmät, asianmukainen sijoittaminen ja toiminta. Segmentoinnissa voidaan turvallisuustasoiltaan erilaiset verkot erotella toisistaan tietoliikennetekniikoiden avulla. Segmentointia tehdään sekä fyysisellä että loogisella tasolla. Fyysinen segmentointi voidaan toteuttaa muista erillään olevilla valokuiduilla. Looginen eriyttäminen voidaan tehdä verkon virtualisoinnilla. Viranomaisyhteistyössä tulee kiinnittää huomiota tarkkaan määriteltyihin turvallisuusluokkiin ja toteutukselle määriteltyihin turvallisuusluokan kriteereihin, jolloin verkkojen välille voidaan rakentaa luotettavia ja turvallisuusluokitukset täyttäviä yhdyskäytäväratkaisuja.

Nykyisin yritysten toimipisteitä, konesaleja ja pilvipalveluita yhdistetään pääasiassa SD-WAN (Software Defined Wide Area Network) -teknologialla, joka käyttää ohjelmistopohjaista verkkotekniikkaa, kuten internetin kautta tapahtuvaa tiedonsiirtoa päällekkäisten salattujen tunnelien avulla. Sillä voidaan toimipaikkojen välinen tietoliikenne toteuttaa turvallisesti, koska kaikki liikenne verkon reunalaitteiden ja -pisteiden välillä salataan. SD-WAN mahdollistaa verkon hallinnan keskitetysti.

**Lohkoketjuteknologia voi toimia** myös turvallisuutta lisäävänä elementtinä viestintäverkoissa. Lohkoketjun tekniikassa toisilleen vieraat toimijat voivat yhdessä tuottaa ja ylläpitää tietokantoja hajautetusti. Tekniikan ansiosta ketjun jäsenet voivat luottaa toisiinsa, vaikka he eivät tuntisi toisiaan. Lohkoketju lisää luottamusta, kun tietokantaa ylläpidetään ilman tietokantaa hallinnoivaa auktoriteettia. Jokaisella verkon toimijalla on pääsy näkemään lohkoketjun sisältö ja jokainen transaktio tallentuu todistettavasti sekä turvallisesti lohkoketjuun. Lisäksi tieto on myös jäljitettävissä. Lohkoketjun hyötynä on myös, että tietokanta on hajautettuna samanaikaisesti useaan eri paikkaan, jolloin sitä on vaikea väärentää. Konsensuksen saavuttamiseksi muodostetaan konsensusalgoritmi erilaisiin käyttötarkoituksiin. Lohkoketjuteknologialla voidaan parantaa yhteiskunnan kriittisten tietovarantojen (esim. Kela, DVV) turvallisuutta ja torjua datamanipulaatioon perustuvia kyberhyökkäyksiä.

## 4.5 Sääntelyn tehokas implementaatio

**Lopuksi on tärkeää mainita** myös sääntely ja lainsäädäntö. NIS2-direktiivissä velvoitetaan kriittiseen infrastruktuuriin kuuluviksi katsotut toimijat täyttämään tietyt kyberturvallisuuteen liittyvät kriteerit, mikä luonnollisesti tarkoittaa, että nämä kriteerit on pidettävä mielessä tulevaisuuden viestintäjärjestelmiä suunniteltaessa. Direktiivissä vaaditaan järjestelmien suojaamista, pääsyn rajoittamista, erottamista muista järjestelmistä sekä säännöllisiä päivityksiä. Toimijan on myös pystyttävä jatkamaan toimintaansa vakavien häiriöiden ja poikkeusolojen aikana. On lisäksi seurattava CER-direktiivin soveltamista, jonka on tapahduttava kansallisesti heinäkuuhun 2026 mennessä ja joka asettaa lisävastuita toimijoille, joita se koskee.

# 5 Resilienssi ja toimitusvarmuus

**Resilienssi ei myöskään rajoitu** vain fyysiseen infrastruktuuriin. Digitaalisen resilienssin merkitys jätetään edelleen usein huomiotta, mutta nykyaikaisessa digitalisoituneessa yhteiskunnassa se on olennainen osa turvallisuutta. Digitaalisen resilienssin tavoitteena on kyky ylläpitää toimintaa poikkeusoloissa mahdollisimman vähäisillä muutoksilla. Ideaalitilanteessa tämä on otettu huomioon jo järjestelmän suunnitteluvaiheessa. Jos järjestelmä on kuitenkin jo olemassa, on tärkeää tunnistaa palvelun jatkuvuuden kannalta kriittisimmät osat ja se, miten järjestelmä reagoi häiriötilanteisiin. Jos järjestelmä on kriittinen eikä se pysy toiminnassa häiriön aikana, sitä on parannettava. Etenkään niin kutsuttuja ”single point failure” -vikoja, eli koko järjestelmän hajotessaan lamauttavia komponentteja, ei voida jättää huomiotta.

Eräs keskeinen huomioimisen arvoinen näkökohta on järjestelmän kriittisten komponenttien, kuten palvelimien ja arkistojen, fyysinen sijainti. Jos ne sijaitsevat samassa maassa kuin palvelu, järjestelmä voi pysyä toiminnassa myös silloin, jos yhteys muihin maihin katkeaa. Jos taas kriittiset palvelut ovat esimerkiksi ulkomaisessa pilvipalvelussa, yhteyden katkos voi poistaa järjestelmän kokonaan käytöstä. Tämä pätee myös siinä tapauksessa, että vain yksi kriittinen palvelu ei ole käytettävissä. Tästä syystä on myös tärkeää, ettei kaikessa ole riippuvainen yhdestä palveluntarjoajasta, koska häiriö heidän palveluissaan johtaisi silloin koko järjestelmän romahtamiseen.

**Digitaalisen resilienssin merkitys jätetään edelleen usein huomiotta, mutta nykyaikaisessa digitalisoituneessa yhteiskunnassa se on olennainen osa turvallisuutta.**

# 6 Pilviteknologian merkitys resilienssin rakentamisessa

**Globaali muutos** pois paikallisista toimijoista kohti pilvipalveluita on kiihtymässä. Tämän ansiosta lähes kuka tahansa voi pian rakentaa oman mobiiliverkkonsa. On myös tiettyjä riskejä, jotka liittyvät riippuvuuteen niin sanotuista hyperskaalaajista, kuten Googlesta, Amazon Web Servicestä ja Microsoftista. Amerikkalaiset tuotteet eivät ole täysin luotettavia poliittisen eskaloitumisen riskin takia, kuten hiljattain nähtiin, kun Microsoft esti pääsyn tuotteisiinsa tietyiltä ICC:n jäseniltä presidentti Trumpin pakotteiden vuoksi. Pilvipalvelutkaan eivät ole immuuneja näille riskeille, joten palveluntarjoajia on arvioitava huolellisesti. Suomen lainsäädäntö myös rajoittaa nimenomaan tällaisia riippuvuuksia, joten tavanomaisilla operaattoreilla on varmasti rooli myös tulevaisuudessa. Kilpailu hyperskaalaajien kanssa tulee kuitenkin olemaan erittäin kovaa, joten operaattorit tulevat kohtaamaan monia haasteita.

Pilviteknologiat voisivat parantaa joustavuutta ja mahdollistaa useampien kaksikäyttötuotteiden helpon integroimisen puolustusratkaisuihin samalla, kun taktinen reunalaskenta parantaa entisestään joustavuutta ja varmistaa, etteivät yhteydet ylikuormitu. Pilvipalvelut voisivat siis olla yksi osa ratkaisua joustavampien järjestelmien ja rakenteiden kehittämiseen. Pilviverkkojen skaalautuvuus voisi mahdollistaa ennennäkemättömän tilannetietoisuuden, autonomisten järjestelmien tuen, reaaliaikaisen kohteen seurannan ja tehokkaammat simulointityökalut.

Tämä edellyttää kuitenkin muutoksia sekä asenteisiin pilvi-integraatiota kohtaan että toimintamalleihin sen käyttöönoton yhteydessä. Sotilaallisten järjestelmien erottaminen kokonaan muista järjestelmistä voi olla keskeinen vaatimus. Se edellyttäisi edelleen erittäin perusteellista auditointiprosessia sekä alkuperäisille järjestelmille että mahdollisille muille pilvipalveluihin liitettäville laitteille, mukaan lukien mahdolliset kaksikäyttöjärjestelmät. Kaikkea ei kuitenkaan voida ratkaista pilvipalveluilla. Vaikka pilvijärjestelmä olisi täysin erillinen, tietoturva on suuri huolenaihe, ja salaiset tiedot on ehkä parasta pitää kokonaan poissa pilvestä. Siksi myös perinteisten viestintäratkaisujen tarve säilyy.

# 7 Satelliittiteknologioiden rooli korostuu

**Toinen keskeinen viestintäteknologia** ovat satelliitit, joiden käyttö on kasvanut räjähdysmäisesti muutaman viime vuoden aikana. Tällä hetkellä monet suuret ja pienet satelliittiviestinnän toimijat ovat yhdistämässä voimansa tarjotakseen asiakkailleen laajemman palveluvalikoiman. Kun otetaan huomioon uudet geopoliittiset olosuhteet, joissa redundanssin (varajärjestelmien olemassaolo vikatilanteita varten, jolloin toiminta ei keskeydy), häiriönsietokyvyn, monikiertoradan, monikaistaisuuden ja viestinnän turvallisuuden kaltaiset käsitteet ovat nousemassa kuumiksi puheenaiheiksi sekä tekoälyn, paikkatietotiedustelun ynnä muiden vastaavien teknologiset edistysaskeleet, on strateginen etu pystyä tarjoamaan asiakkailleen laajempi valikoima palveluja erityisesti silloin, kun on kyse kaksikäyttöjärjestelmistä.

Monet satelliitti- ja televiestintäyritykset keskittyvät direct-to-cell-yhteyteen visionaan tarjota saumaton yhteys asiakaskunnalleen. Tällä hetkellä kehitteillä on kaksi pääsuuntaa: verkon pyörittäminen matkapuhelinoperaattorin spektrillä "avaruudessa olevien tukiasemien" kautta ja kumppanuudet teleoperaattoreiden kanssa – tätä Starlinkin, Lynk Globalin tai AST SpaceMobilen kaltaiset organisaatiot rakentavat tällä hetkellä. Tämän ratkaisun keskeinen etu on, että nykypäivän älypuhelimet on jo viritetty maanpäällisille radioaalloille, mikä tarkoittaa, ettei uuden sukupolven matkapuhelimia tarvitse odottaa, jotta tekniikka olisi käyttökelpoinen.

**Toinen vaihtoehto** on kehittää erillisiä direct-to-phone-konstellaatioita, jotka toimivat mobiilisatelliittien taajuudella (pääasiassa L-kaistalla). Käyttämällä taajuuksia, jotka on jo hyväksytty lähetettäväksi avaruudesta maahan, lyhennetään kaupalliseen laukaisuun kuluvaa aikaa, koska ylimääräisiä lupia tai kumppanuuksia ei teknisesti tarvita. Tämä kuitenkin vaatii, että kuluttajat käyttävät uusimpia matkapuhelimia, joissa on seuraavan sukupolven siruja. Tulevaisuuteen katsottaessa tämä näyttää todennäköisemmältä vaihtoehdolta pitkällä aikavälillä, koska uusien laitteiden käyttöönotto ei silloin ole ongelma. Kaksikäytön osalta tämä näyttää myös todennäköisemmältä vaihtoehdolta, koska se tarjoaa paremman mahdollisuuden erottaa sotilaallinen viestintä tavallisista matkapuhelimista.

Tämän muutoksen eturintamassa on ei-maanpäällisten verkkojen (non-terrestrial-network, NTN) ilmaantuminen. Kyseiset verkot kiertävät nimensä mukaisesti täysin perinteisen maainfrastruktuurin. Nykyään satelliittiorganisaatiot mahdollistavat nopean yhteyden jopa maailman syrjäisimmille ja alipalvelluille alueille tarjoamalla yhteyksiä avaruudesta. Tämä on jo

osoittautunut kriittiseksi Ukrainan sotilaallisen komentorakenteen kannalta, eikä vaadi kovin suurta mielikuvitusta kuvitella, kuinka tärkeitä NTN:t ovat alueilla, joilla kriittinen infrastruktuuri maassa on osittain tai kokonaan tuhoutunut.

On sanomattakin selvää, että NTN:istä tulee tulevaisuudessa lähes pakollinen varajärjestelmä sekä siviili- että sotilasviestinnälle kriisien aikana. Satelliittipohjaiset ratkaisut olisivat kenties paras mahdollinen varajärjestelmä myös suomalaiselle viranomaisviestinnälle, sillä perinteinen radioverkko on helpompi tuhota kriisitilaneessa etenkin silloin, jos edes osa tukiasemista on muiden verkkojen tukiasemien läheisyydessä. Puolustusvoimat on muutenkin panostamassa lähivuosina avaruusteknologiaan uuden avaruuskomentajansa johdolla, joten kommunikaatiojärjestelmät voisivat olla luonnollinen osa tätä kehitystä.

**Satelliittijärjestelmät tarjoavat** mahdollisuuden tuottaa nopeita sekä lyhyen viiveen internet- ja datapalveluja paikoissa, jotka ovat kaukana maanpäällisen infrastruktuurin ulottumattomissa, kuten avoimilla vesiväylillä, maaseutukylissä, vuorilla ja katastrofialueilla. Tämä luonnollisesti pätee myös konfliktialueisiin. Satelliittioperaattorit luovat luotettavia, skaalautuvia ja rajattomia järjestelmiä, jotka poistavat maainfrastruktuurin tarpeen ja mahdollistavat kaiken kansallisesta logistiikasta hätäapuun. NTN:t tarjoavat yhteyksiä ylhäältä päin, toisin kuin perinteiset maanpäälliset verkot, jotka edellyttävät tiheää infrastruktuuria ja ovat joko kalliita tai epäkäytännöllisiä ottaa käyttöön syrjäisillä tai vaarallisilla alueilla. Ne antavat yrityksille erinomaisen mahdollisuuden auttaa alipalveltuja yhteisöjä kaikkien poliittisten ja maantieteellisten rajojen yli. Lisäksi NTN-verkot mahdollistavat satelliittien ja korkealla lentävien alustojen (High Altitude Platform Station, HAPS), kuten ilma-aluksiin sijoitettujen tuki- tai toistinasemien, toiminnan rinnakkain maa-asemaverkkojen kanssa. HAPS-ratkaisut voisivat tukea kiinteää laajakaistaa loppukäyttäjille sekä toimia transmissiolinkkinä mobiiliverkkojen ja kiinteän verkon välillä.

Satelliittikonstellaatioihin on rakennettu redundanssi- ja mesh-reititysominaisuuksia, jotka parantavat verkon joustavuutta ja vähentävät yksittäisiä vikapisteitä. Konstellaatiot yhdessä tekoälypohjaisen liikenteen reitittämisen ja autonomisten lentokoneiden kanssa laajentavat kattavuutta ja edistävät siirtymistä mukautuviin verkkomalleihin. On varsin selvää, miten nykyiset teknologiatrendit voivat muodostaa lumipalloefektin: kvanttilaskenta lisää tekoälyn valmiuksia, mikä puolestaan nopeuttaa tutkimusta kaikilla osa-alueilla, mukaan lukien satelliittiviestintä, reunalaskenta ja pilvipalvelut, jotka laajentavat verkkojen kattavuutta kaikkialle maapallolle. Perinteisellä maanpäällisellä infrastruktuurilla on kuitenkin edelleen tärkeä rooli, koska sillä on joitain etuja satelliittipohjaisiin ratkaisuihin verrattuna. Satelliitteja on järkevintä käyttää ensisijaisesti syrjäisillä alueilla ja varatoimenpiteenä siltä varalta, että maanpäällinen infrastruktuuri vaarantuu.

**Satelliittipaikannus on keskeinen** osa yhteiskunnan toimintaa ja tämän päivän sodankäyntiä. GNSS (Global Navigation Satellite System) tarjoaa käyttäjille paikannus-, navigointi- ja ajoituspalveluita (positioning, navigation, timing, PNT). GNSS-järjestelmien häirintä ja spoofing Venäjän ja Ukrainan sodassa osoittavat järjestelmän haavoittuvuuden ja myös vaikutusten leviämisen hyvinkin laajalle alueelle. GNSS-häirinnänestojärjestelmät toimivat havaitsemalla, lieventämällä ja joissakin tapauksissa täysin neutraloimalla häirintäsignaalien vaikutuksia varmistaen GNSS-pohjaisten palvelujen luotettavuuden ja tarkkuuden. Nämä palvelut ovat kriittisiä erityisesti ympäristöissä, joissa luotettava navigointi ja paikannus ovat ratkaisevan tärkeitä, kuten sotilasoperaatioissa, ilmailussa, merinavigoinnissa, autonomisissa ajoneuvoissa ja kriittisessä infrastruktuurissa. Käyttämällä erilaisia menetelmiä, kuten antenniryhmiä, edistyneitä signaalinkäsittelyalgoritmeja ja adaptiivista suodatusta, GNSS-häirinnänestojärjestelmät auttavat suojautumaan häirinnän aiheuttamilta mahdollisilta uhilta ja ylläpitämään GNSS-palveluiden jatkuvaa saatavuutta.

**Satelliitteja on järkevintä käyttää ensisijaisesti syrjäisillä alueilla ja varatoimenpiteenä siltä varalta, että maanpäällinen infrastruktuuri vaarantuu.**

# 8 Kansallisen resilienssin vahvistaminen

**Kun Ukrainasta ja muualta** saadut opit yhdistetään nousevan teknologian mahdollisuuksiin, voidaan löytää ratkaisuja kriittisen viestinnän tulevaisuuden haasteisiin moderneissa yhteiskunnissa. Tulevaisuuden kriittisen infrastruktuurin kenties tärkein vaatimus kiteytyy digitaaliseen ja fyysiseen resilienssiin. Erityisesti Ukrainasta saatuihin kokemuksiin perustuen tähän resilienssiin tulisi sisältyä kestävyys elektronisen sodankäynnin operaatioita vastaan.

Järjestelmät on tietysti suojattava hyvin, mutta täysin toimintavarmaa järjestelmää ei ole olemassa. Kun jokin lopulta menee pieleen, käytettävissä on oltava varajärjestelmiä, ja alkuperäisen laitteiston tai järjestelmän korjauksen tai vaihdon on tapahduttava nopeasti. Tämän helpottamiseksi on tarpeen varmistaa, että komponentit ja henkilöstö ovat riittävän lähellä nopeaa reagointia varten. Kaksikäyttöjärjestelmät ovat yksi keino saavuttaa tämä tavoite, koska henkilöstön asiantuntemusta ja vaihdettavia komponentteja voidaan siten lainata siviilijärjestelmistä sotilasjärjestelmiin ja päinvastoin. Varajärjestelmien puuttumisen aiheuttamista ongelmista esimerkkinä on Venäjän toteuttaman GPS-häirinnän vaikutus lentoliikenteeseen. Osassa lentokenttiä ei ole enää varajärjestelmiä, ja jos GPS ei toimi, joudutaan lento keskeyttämään, kuten tapahtui Suo-

**Tulevaisuuden kriittisen infrastruktuurin kenties tärkein vaatimus kiteytyy digitaaliseen ja fyysiseen resilienssiin.**

messa ja Virossa. Suomessa onkin otettu käyttöön korvaavia järjestelmiä ja tutkapalvelua lähestyville koneille.

**Kaksikäyttöjärjestelmät tuovat** myös haasteita. Siviilituotteiden sotilaallisen käytön riittävän turvallisuuden varmistaminen on niistä suurin. Järjestelmien testaaminen ja niiden kanssa harjoittelu voi myös osoittautua haastavammaksi kuin puhtaasti sotilaallisia järjestelmiä käytettäessä, mutta onneksi Suomessa on pitkä historia tiiviistä yhteistyöstä armeijan ja muun yhteiskunnan välillä. Yhteistyön yksityisen ja julkisen sektorin toimijoiden välillä onkin oltava saumatonta, ja esimerkiksi Ukrainassa toimivaksi todetun operaattoreiden välisen verkkovierailemisen valmistelu olisi hyvä toteuttaa jo normaalioloissa parhaan mahdollisen reaktionopeuden saavuttamiseksi. Ylimääräiset poliittiset esteet resilienssille tulisi niin ikään kitkeä pois luotettavia yrityskumppanuuksia solmittaessa. Vain yritysten ja julkisen sektorin yhteisellä monitoimijamallilla on mahdollista varmistaa digitaalinen suvereniteetti myös poikkeusoloissa.

Jo saatavilla olevista teknologioista satelliitti- ja pilvijärjestelmät ovat merkittävimpiä, kun kuvitellaan ratkaisuja edellä mainittuihin vaatimuksiin. Pilvijärjestelmät voivat tarjota mahdollisuuden yhdistää organisaation eri osat dynaamisesti ja kustannustehokkaasti toisiinsa lähes rajattomalla skaalautuvuudella säilyttäen samalla mahdollisuuden segmentointiin. Yhdistettynä tekoälyn kehitykseen pilvijärjestelmien mahdollisuudet ovat lähes rajattomat autonomisten järjestelmien tuesta reaaliaikaiseen kohteen seurantaan. Ne ovat myös tehokas tapa parantaa fyysistä häiriönsietokykyä, sillä vahingoittunut infrastruktuuri yhdessä paikassa ei välttämättä tarkoita palvelujen saatavuuden menettämistä, varsinkaan yhdistettynä satelliittiyhteyksiin. NTN:ien avulla voidaankin varmistaa, että verkkoyhteydet ovat aina käytettävissä kaikkialla maanpäällisen infrastruktuurin tilasta riippumatta. Niistä voi myös tulla melko tehokas ratkaisu viestinnän tarjoamiseen syrjäseuduille, joista puuttuu vielä maanpäällisiä verkkoja.

**Pilviratkaisujen lisäksi** tekoäly mullistaa todennäköisesti myös monia muita aloja varsinkin silloin, kun kvanttilaskenta kehittyy vaiheeseen, jossa sitä voidaan käyttää tekoälyn voimanlähteenä. Julkisten arvioiden mukaan se tapahtuu mahdollisesti jo seuraavan viiden vuoden aikana. Siksi tarvitaan kokonaisvaltaista sys-

teemiajattelua rakennettaessa resilienttiä kansallista kommunikaatiojärjestelmää. Tällaisessa ”System of systems” -ajattelussa hahmotetaan kokonaisuuksia, jotka koostuvat useista toisiinsa kytkeytyvistä järjestelmistä. Lähestymistavassa ei tarkastella vain yksittäisiä järjestelmiä, vaan niiden keskinäisiä vuorovaikutuksia ja yhteisvaikutuksia, jotta voidaan ymmärtää kokonaisuuden toimintaa ja kehittää uusia, entistä tehokkaampia ratkaisuja.

Tarvitaan usean kommunikaatioteknologian joustavaa ja monikerroksista käyttöä. Yhteiskunnan kriittisen informaatioinfrastruktuurin tulee rakentua kiinteiden ja mobiili- ja satelliittiteknologioiden yhteiseen verkostomaiseen käyttöön. Valokuituyhteyksillä voidaan tuottaa suuria siirtonopeuksia (kaupalliset systeemit 100 Tbps, tutkimuslaboratorioissa yli 400 Tbps) ja ne tulisi liittää saumattomasti 5G-verkkoihin. Uusin valokuituteknologia sisältää kvanttimekaniikkaan perustuvia menetelmiä, jotka varmistavat turvallisen tiedonsiirron. Lisäksi tekoälyanalytiikkaa ja -automaatiota integroidaan kuituverkkoihin verkon suorituskyvyn parantamiseksi, kaistanleveyden optimoimiseksi ja viantunnistuksen tehostamiseksi. Kuituoptisten kaapelikokoonpanojen rooli automaatiossa yhdessä langattomien järjestelmien kanssa tulee kasvamaan. Erityisesti sitä tarvitaan tehtaissa ja varastoissa, joissa käyttöön otetaan robotiikkaa ja autonomisia tuotantotapoja. Langalliset ja langattomat järjestelmät lisäävät redundanssia ja systeemien resilienssiä.

**Tulevaisuuden järjestelmien** on myös oltava helposti muokattavia, koska toimintaympäristö on jatkuvassa muutoksessa. Tämä näkyy ehkä parhaiten Ukrainassa, jossa droonien kehityssykli kiihtyy ja kiihtyy. Kehitys eri teknologia-alueilla kuten kvantti, tekoäly, 5G/6G, satelliitti, pilvipalvelut ja valokuitu sekä niiden vaikutus kaikkiin muihin järjestelmiin tarjoavat myös ainutlaatuisia mahdollisuuksia ja haasteita viestintäjärjestelmille. Siksi on ehdottoman tärkeää kiinnittää huomiota näiden keskeisten valmiuksien kehitykseen lähitulevaisuudessa. Kyky mukauttaa jo käytössä olevia järjestelmiä uusiin innovaatioihin ja käyttötapauksiin on valtava etu sekä taloudellisesti että ajallisesti verrattuna kokonaan uusien laitteiden ja ohjelmistojen hankkimiseen aina, kun uusia ominaisuuksia kehitetään. Kaksikäyttöjärjestelmätkin ovat huomattavasti houkuttelevampia, jos niitä voidaan nopeasti ja helposti muokata sopimaan paremmin sotilaallisiin käyttötapauksiin sotilaallisessa käytössä ja siviilikäyttöön siviilikäytössä.

Kansallisessa kriittisessä infrastruktuurissa data on toiminnan keskiössä. Datataloudessa eri toimijat (kansalaiset, yritykset, julkiset organisaatiot) työskentelevät yhteisessä ympäristössä datan saannin, siirron ja käytettävyyden varmistamiseksi sekä hyödyntävät dataa ja luovat siten uusia innovaatioita ja palveluita. Datan siirto eri toimijoiden välillä on keskeinen osa viestintää ja digitaalisten järjestelmien toimintaa. Kriittisen infrastruktuurin toimijoiden tulee rakentaa verkottunut, vaihtoehtoisia tiedonsiirtomuotoja ja kehittyneitä teknologioita käyttävä kyberturvallinen kokonaisuus, jolla saavutetaan tarvittavaa resilienssiä toiminnan eri tasoilla. Samalla tulee huolehtia dataan liittyvän regulaation tehokkaasta implementoinnista.

**Kyky mukauttaa jo käytössä olevia järjestelmiä uusiin innovaatioihin ja käyttötapauksiin on valtava etu sekä taloudellisesti että ajallisesti verrattuna kokonaan uusien laitteiden ja ohjelmistojen hankkimiseen aina, kun uusia ominaisuuksia kehitetään.**

# LÄHTEET:


https://www.comsoc.org/publications/ctn/predicting-future-communications-technologies

https://www.hs.fi/alueet/art-2000011306235.html

https://www.avenga.com/magazine/satellite-technology-bringing-satellite-in-the-palm-of-the-hand/

https://satcube.com/news/current-satcom-trends-shaping-the-future-of-connectivity?gad_source=1&gad_campaignid=21079435382&gclid=EAIaIQobChMIpNOMseiijgMVvluRBR1C2iy1EAAYASAAEgICY_D_BwE

https://www.techtarget.com/searchdatacenter/definition/edge-computing

https://www.telekom.com/en/company/management-unplugged/details/satellite-communication-a-powerful-addition-to-europe-s-digital-future-1093760

https://spacenews.com/shaking-up-satcom-the-time-is-now-for-radical-innovation-in-satellite-communications/

https://www.critical-entities-resilience-directive.com/

https://www.telia.fi/yrityksille/artikkelit/artikkeli/tutustu-digitaaliseen-huoltovarmuuteen

https://gofore.com/kuka-suojelee-meita-kriisissa-jossa-kysytaan-digitaalista-huoltovarmuutta/

https://www.dna.fi/yrityksille/blogi/-/blogs/5g-ssa-voit-viipaloida-yritysverkkosi-mita-se-kaytannossa-tarkoittaa

https://thebulletin.org/2025/03/russian-networks-flood-the-internet-with-propaganda-aiming-to-corrupt-ai-chatbots/

https://viestiupseeriyhdistys.fi/wp-content/uploads/2021/08/VM-2-2021.pdf

https://viestiupseeriyhdistys.fi/lehti/viestimies-4-2023/

https://issuu.com/viestimies/docs/vm_2024-1

https://issuu.com/viestimies/docs/viestimies_1_2025/30

https://issuu.com/viestimies/docs/viestimies_2_2025

https://ai-ran.org/

https://www.erillisverkot.fi/virve2-0/?gad_source=1&gad_campaignid=16178890739&gclid=EAIaIQobChMI8ontv6PQjwMVNQiiAx3n2Bf-EAAYASAAEgJvh_D_BwE

Cyberwatchin analyysi Ukrainan sodasta

Cyberwatchin viikkokatsaukset

Kyberaamiaisen 2025 esitykset

# MEIDÄT LÖYTÄÄ

**Uudistetuilta kotisivuilta**

www.cyberwatchfinland.fi

**LinkedInistä**

www.linkedin.com/
company/cyberwatchfinland

**Instagramista**

https://www.instagram.com/
cyberwatchfinland/

***Seuraamalla meitä saat tietoa uusista julkaisuistamme, kyberturvallisuuden tapahtumista sekä vinkkejä kyberturvallisuuden kehittämiseen.***

# Tavoitteena kyberkyvykkäämpi maailma


## Ota yhteyttä

Cyberwatch Oy | Nuijamiestentie 5 C | 00400 Helsinki, Finland
aapo@cyberwatchfinland.fi | info@cyberwatchfinland.fi | 040 500 8177