

Asia: VN/6290/2025

Turvallisuutta ja uutta talouskasvua tietoverkoista -hanke (TUUTTI-hanke)

Kysymykset

Mitkä teknologiset, taloudelliset, geopoliittiset ja muut yhteiskunnalliset muutokset ovat keskeisimpiä viestintäverkkojen kehityksen kannalta seuraavan kymmenen vuoden aikana?

Teknologisista muutoksista keskeisin on siirtyminen PQC- eli post-quantum cryptography -aikaan. Esim. EU:n uuden PQC-tiekartan mukaan kaikkien jäsenvaltioiden pitää aloittaa siirtymä post-quantum -aikaan vuoden 2026 loppuun mennessä, ja kriittisten infrastuktuurien osalta viimeistään v. 2030 loppuun mennessä. Siirtymä on välttämätön erityisesti viestintäinfrastruktuurien pitkäaikaisen turvallisuuden takaamiseksi.

Teknologinen kehitys (kuten lohkoketjut ja Zero Trust) on johtanut hajautettujen turvallisuusarkkitehtuurien yleistymiseen. Hajautetut järjestelmät vähentävät riippuvuutta kolmannen osapuolen jatkuvalle luotolle ja mahdollistavat datan ja pääsynhallinnan säilymisen käyttäjän hallussa myös offline-tilassa tai kriisitilanteissa. Viestintäverkkojen kyseessä ollen tämä on erityisen tärkeää. Hajautettujen verkkojen vahvuudet ovat erityisesti toimintavarmuus, skaalautuvuus ja luottamuksen rakentaminen verkon eri osapuolten välillä.

Hajautettu verkko ei ole riippuvainen yksittäisestä keskuskomponentista, jolloin se kestää paremmin vikatilanteita, palvelunestohyökkäyksiä tai muita häiriöitä. Tämä on erityisen tärkeää kriittisissä palveluissa, joissa verkon jatkuva toiminta on välttämätöntä. Hajautettu arkkitehtuuri mahdollistaa verkon laajentamisen ilman, että koko infrastruktuuria tarvitsee keskitetysti uudelleenrakentaa. Lisäksi verkkojen ääripäät (esim. reunalaskenta ja IoT-solmut) voivat tehdä päätöksiä paikallisesti tehokkaammin. Hajautus mahdollistaa todennettavan luottamuksen useiden toimijoiden välillä ilman, että kaikkien tarvitsee luottaa samaan yksittäiseen keskitettyyn osapuoleen. Tämä on keskeistä esimerkiksi tilanteissa, joissa verkon osapuolet edustavat eri organisaatioita tai maita. Hajautetut verkot tukevatkin periaatetta, jossa verkon käyttäjät ja operaattorit voivat rakentaa ja hallita omia osiaan riippumatta ulkopuolisista tahoista, vähentäen näin toimittajariippuvuutta ja tukien digitaalista suvereniteettia.

Viestintäverkkojen ohjelmallinen hallinta (esim. SDN, Zero Trust, AI-ohjaus) edellyttää uudenlaisia turvallisuusmalleja. Ohjelmallisesti määriteltävät verkot mahdollistavat politiikkapohjaisen liikenteen ja pääsyoikeuksien hallinnan, ts. päätös siitä, voiko käyttäjä tai laite liittyä verkkoon tehdään dynaamisesti eikä staattisten sääntöjen perusteella. Samalla pääsynhallinnan turvallisuuden takaaminen korostuu.

Tekoälyn vaikutusta kaikkeen teknologiaan liittyvänä muutoksena ei voi aliarvioida. Tekoäly tuo viestintäverkoille merkittäviä mahdollisuuksia turvallisuuden, suorituskyvyn ja resilienssin kehittämisessä. Se mahdollistaa dynaamisen reagoinnin uhkiin, itsenäisen verkonhallinnan ja käyttäjälähtöisen optimoinnin. Samanaikaisesti sen käyttö vaatii vahvaa läpinäkyvyyttä, hajautettua toteutusta ja sääntelyn huomioimista.

Geopolitiikan kannalta keskeistä on turvata Euroopan digitaalinen suvereniteetti eli kyky suojata viestintää ilman ulkopuolisia riippuvuuksia. Tähän liittyy vahvasti myös datasuvereniteetti, eli Eurooppalaisten henkilötietojen säilyttäminen omassa hallinnassa. Viimeaikaiset Microsoft-uutisoinnit toisaalta Kansainvälisen rikostuomioistuimen ICC:n syyttäjän sähköpostiyhteyksien katkaisemisesta Euroopassa ja toisaalta yhtiön oman lakimiehen lausunto siitä, etteivät eurooppalaisten henkilötiedot olisi ”turvassa” Euroopassa, puoltavat eurooppalaisten ratkaisujen käyttöönottoa ja irtaantumista US-riippuvuudesta.

Myös kauppapolitiittiset näkökannat puoltavat Euroopan teknologiasuvereniteetin varmistamista. Kauppapolitiikka on keskeinen osa geopolitiittista toimintaympäristöä, joka vaikuttaa suoraan viestintäverkkojen kehittämiseen. Kansainväliset vientirajoitukset, teknologiasääntely ja pilvipalveluiden alueellistaminen luovat sekä esteitä että kannustimia kotimaisten ja eurooppalaisten turvallisuus- ja viestintäteknologioiden kehitykselle sillä erityisesti tietoturvalliset komponentit, kvanttiturvallinen kryptografia, viestintälaitteet ja ohjelmistot voivat joutua vientirajoitusten piiriin (esim. USA:ssa EAR).

Maailman epävakaa turvallisuustilanne – erityisesti Euroopassa – on geopolitiittinen kehityskulku, joka vaikuttaa suoraan turvallisen viestintäinfrastruktuurin strategiseen merkitykseen. Samalla sen heijastumat ulottuvat yhteiskunnan toimintaedellytyksiin, palveluiden jatkuvuuteen ja kansalaisten luottamukseen. Luottamus viestintään edellyttää läpinäkyvää mutta yksityisyyttä kunnioittavaa infrastruktuuria. Yhtäältä yhteiskunnallisena muutoksena voikin nähdä juuri yksityisyyden suojan korostamisen mutta toisaalta tarpeen suojella esim. lapsia verkossa ja viestisovelluksissa liikkuvalla sopimattomalla sisällöllä. Tarvitaan uudenlaisia turvallisuusratkaisuja, jotka mahdollistavat sekä salatun viestinnän että sopimattoman tai esim. terrorismiin liittyvän sisällön havaitsemisen salatusta sisällöstä.

Mitä konkreettisia tarpeita ja teemoja tulisi tarkastella entistä turvallisempien ja talouskasvua luovien viestintäverkkojen ja teknologian kehittämiseksi?

Teknologia-agnostisuus ja mukautuvuus uuteen teknologiaan

Viestintäverkkojen tulee tukea pitkäaikaisesti kestäviä suojausratkaisuja, ilman riippuvuutta tietyistä teknologioista ja/tai toimittajista. Turvallisuusratkaisujen tulee olla joustavia ja kyetä mukautumaan teknologiseen muutokseen ilman infrastruktuurin uudelleenrakentamista (kryptografinen ketteryys).

Huoltovarmuus

Viestintäverkoissa on kyettävä toimimaan myös tilanteissa, joissa yhteydet katkeavat tai ympäristö on poikkeuksellinen (hajautetun arkkitehtuurin ja vaihtoehtoisten yhteysteknologioiden merkitys). E erityisen kriittistä huoltovarmuuden kannalta on viranomaistoiminnan nojautuminen kriittisessä viestinnässä ohjelmistoihin tai päätelaitteisiin, joiden hallinta tai jakelualusta on ulkomaisen sääntelyvallan piirissä.

Mitä kehityksen esteitä, riskejä tai uhkia Suomessa ja Euroopassa on uusien digitalisaatioon nojaavien käyttökohteiden, liiketoiminnan ja sektoreiden kehitykselle sekä näitä tukevien investointien ja innovaatioiden syntymiselle?

Digitalisaation mahdollistamat uudet käyttökohteet, liiketoiminta-alueet ja palvelut vaativat tuekseen ennakoitavaa sääntely- ja investointiympäristöä, teknologista kapasiteettia sekä kansainvälistä kilpailukykyä. Ylisääntely vaikeuttaa digitaalisten palveluiden kehitystä Euroopassa ja heikeintää Euroopan kilpailukykyä.

Toimittajariippuvuus (vendor lock-in): Monet organisaatiot ovat kiinni PKI-infrastruktuurissa ja kansainvälisissä CA-järjestelmissä. Tämä jarruttaa siirtymää hajautettuihin ja suvereenimpiin malleihin.

Ulkomaaiset toimijat ja vieraan valtion vaikutus. Euroopan digitaaliset palvelut nojaavat edelleen vahvasti ulkomaiseen infrastruktuuriin (esim. pilvipalvelut). Tämä vaikeuttaa digitaalista suvereniteettia, heikentää toimitusvarmuutta ja rajoittaa turvallisuuskriittisten sovellusten itsenäistä kehittämistä.

Uudet käyttökohteet edellyttävät horisontaalista yhteistyötä eri liiketoimintasektoreiden välillä. Toimialakohtainen siiloutuminen ja epäyhteensopivat järjestelmät estävät skaalautuvien ratkaisujen käyttöönottoa.

Uuden ajan uhat vaativat uudenlaista turvallisuusajattelua. Monet olemassa olevat järjestelmät eivät ole suunniteltu estämään esim. hybridioperaatioita, kvanttiteknologiaa tai tekoälyavusteisia kyberhyökkäyksiä.

Eurooppaa vaivaa uskalluksen puute uusien, edistyksellisten (disruptive) teknologioiden käyttöönotossa etunenässä. Markkinat suosivat lyhyen aikavälin kannattavuutta ja valmiita ratkaisuja. Tämä voi estää kehittämästä ja käyttöönottamasta sellaisia ratkaisuja, jotka vaativat pitkäjänteistä kehitystä, kuten uudenlaisten turvallisuusarkkitehtuurien rakentaminen tai kvanttiturvallisten teknologioiden kehitys.

Mitkä asiat vaikuttavat siihen, että Suomi on tulevaisuudessakin edistyksellinen maa turvallisten ja luotettavien viestintäverkkojen ja -teknologioiden käytössä?

Suomella olisi tarjota kilpailukykyisiä ratkaisuja EU:n kyberturvallisuuden itsemääräämisoikeuden mahdollistamiseksi. Suomen mahdollisuus vahvistaa asemaansa edistyksellisenä ja luotettavana toimijana viestintäteknologioissa perustuu kuitenkin useiden tekijöiden yhteisvaikutukseen. Kyse ei ole vain teknologisesta kehityksestä vaan myös poliittisesta tahdosta, lainsäädännöllisestä ennakoitavuudesta ja kyvystä toimia osana laajempaa eurooppalaista ja kansainvälistä kokonaisuutta. Tarvitaan pitkäjänteinen ja tavoitteellinen kansallinen kyberturvastrategia sekä yhteensopiva mutta omavarainen teknologiapohja.

Suomeen pitää luoda innovaatiopolitiikka, joka tukee investointeja edistyksellisten teknologioiden kehittämiseen. Myös sääntely-ympäristön pitää mahdollistaa teknologian kehitys ja tukea uusia malleja. Suomen pitää lisäksi ottaa aktiivinen rooli EU-regulaatioiden valmistelussa ja varmistaa, että suomalaiset tarpeet ja arvot huomioidaan kehityksessä.

Turvallisten ja luotettavien viestintäverkkojen kehittäminen edellyttää tiivistä yhteistyötä julkishallinnon, elinkeinoelämän, tutkimusorganisaatioiden ja kansalaisyhteiskunnan välillä. Suomessa yhteistyölle on erityisen hyvät edellytykset verrattuna suurempiin ja hierarkkisempiin maihin. Julkiset toimijat voisivatkin edistää suomalaisten turvallisuusteknologioiden käyttöönottoa hankintojen ja referenssien kautta. Samalla ne tukisivat innovaatioita ja mahdollistaisivat pienemmille toimijoille pääsyn kriittisille markkinoille.

Peräämme uskallusta ottaa käyttöön edistyksellisiä teknologioita ja uskoa kotimaiseen osaamiseen ja teknologiaan. Esimerkiksi Suomen Kyberturvastrategia 2024-2035 sisältää väittämän: ”Kvanttiteknologian nopea kehittyminen haastaa entisestään tämänhetkistä kansallista salauskyykyä. Suomi on jäänyt verrokkimaiden suhteen jälkeen salaustekniikoiden kansallisten ratkaisuiden kehittämisessä.” Näin ei ole. Suomessa on edistyksellisiä teknologioita kehittäviä yrityksiä, jotka eivät vain saa ääntään riittävästi kuuluviin isojen kansainvälisten teknologiajättien jyrätessä ne ylivaltaansa alle. Julkishallinnon on näytettävä esimerkkiä ja asetettava suomalaiset ratkaisut etusijalle. Viemällä suomalaista teknologiaosaamista Eurooppaan luomme turvallisuudesta uutta talouskasvua.

Lummevuo Anne-Mari
Gurulogic Microsystems Oy