

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?

Tekoälyn yleistyminen, palveluiden pilvipohjaisuus, kehittyvä kyberturvallisuus sekä kokonaisvaltainen tietoturva muodostavat keskeisiä teemoja tulevaisuuden tietoverkoissa. Tietoliikenneverkkojen kehityssuunnat painottuvat käyttäjätilipohjaisuuteen sekä matalan latenssin ja suuren kapasiteetin tarjoaviin mobiili- ja kiinteisiin yhteyksiin. Suurena murroksena ovat myös 6G-tekniologian käyttöönotto sekä taajuustoimilupien umpeutuminen, jotka molemmat edellyttävät strategisia ratkaisuja.

Jatkossa varmistettujen maa-, meri- ja ilmareittien sekä fyysisten yhteyksien resilienssi osana kokonaisturvallisuutta sekä kansainvälinen yhteistyö korostuvat entisestään. Kotimainen, pohjoismainen sekä eurooppalainen suvereniteetti näkyy entistä enemmän poliittisessa keskustelussa. Pohjoismainen palvelutuotanto, osaamisen hyödyntäminen sekä turvallisuusselvitysprosessien yksinkertaistaminen ovat tärkeässä roolissa tässä keskustelussa.

Työvoimapula ja teollisen alan osaajien eläköityminen – jonka ennustetaan olevan jopa 30 % vuoteen 2030 mennessä – ohjaa prosesseja kohti vahvaa automaatiota ja tekoälypohjaisia, itseohjautuvia tuotantomalleja. Automaatio ja tekoäly eivät kuitenkaan voi täysin ratkaista osaavan työvoiman haastetta.

Suomeen on suunnitteilla noin 100 uutta konesalia ja Euroopassa on menossa useita gigafactory-hankkeita. Tämä luo merkittävän ekosysteemin kasvun ja innovaatioiden kannalta. Esimerkiksi tekoälyn laskentateho voisi hyvin keskittyä Suomeen mahdollistaen ”uuden Nokian”. Lisäksi datakeskusten kerrannaisvaikutukset ovat pohja kestäväälle kasvulle ja kansalliselle turvallisuudelle. Datakeskuksiin liittyy vahva potentiaali Suomen kilpailukyyn ja huoltovarmuuden vahvistajana.

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

Tarpeettomien tai suhteettomien sääntelyvelvoitteiden poistamisen tulisi olla yleinen tavoite telealan sääntelyssä, eikä sitä tulisi rajoittaa tiettyihin segmentteihin. Haluamme nostaa esille erityisesti yritysliiketoimintaan (B2B) ja koneiden välisiin (M2M)/IoT-palveluihin sovellettavia velvoitteita. Nämä segmentit toimivat erilaisissa kilpailuolosuhteissa kuin perinteiset loppukäyttäjämarkkinat. Suhteellisempi lähestymistapa edistäisi teollisuuden digitalisaation innovaatioita ja vähentäisi hallinnollista taakkaa.

Investointikannusteet tulisi turvata teleoperaattoreille. Käytännössä tätä tavoitetta tukee mahdollisimman ennakoitava sääntelykenttä. Valtaosa Suomen mobiilitaajuustoimiluvista umpeutuu vuonna 2033, toimijoiden tulisi saada varmuus jatkosta hyvissä ajoin etukäteen, jotta verkkojen kehitys jatkuisi saumattomasti ilman epävarmuutta taajuusalueen tulevaisuudesta. Käytännössä viisi vuotta etukäteen olisi toivottava aika, tämä ottaisi huomioon myös tulevan 6G-aikakauden.

Investointikannusteita edesauttaa myös sujuva lupakäytäntö, mukaan lukien lupamaksut. Gigabittiasetuksen tavoitteiden toteutus on tästä yksi konkreettinen esimerkki.

Operaattorien toimintaa ei pitäisi rajoittaa globaalissa alustakilpailussa vaan meidän pitäisi varmistaa SMS:n tyyppisten palveluiden tulevaisuus. Kuluttajille suunnatut viestintäratkaisut, jotka ovat sääntelyn piirissä, edistävät markkinoinnin turvallisuutta. Liian tiukka sääntely on kuitenkin riski, joka voi ajaa toimijoita käyttämään entistä enemmän alustapalveluita. Näitä palveluja ei säännellä yhtä vahvasti, joten taistelu esimerkiksi huijauksia vastaan voi käydä haastavammaksi.

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?

Turvallisuus-, resilienssi- ja telekuuntelun vaatimukset ovat yhä tärkeämpiä nykyisessä uhkaympäristössä, mutta niitä toteutetaan eri tavoin eri puolilla EU:ta. DNA tukee entistä tiiviimpää yhteistyötä tällä alueella. Tavoitteena johdonmukainen soveltaminen EU-tasolla samalla, kun kunnioitetaan kansallisia etuoikeuksia. Ilman tällaista yhdenmukaistamista pirstoutuminen voi vaarantaa sekä tehokkuuden että oikeudenmukaisuuden, erityisesti silloin, kun teleoperaattoreita säännellään eri standardein kuin muita digitaalisen infrastruktuurin tarjoajia.

Ukrainan sota on muuttanut Euroopan turvallisuustilannetta ja tehnyt Pohjoismaiden selviytymiskyvyn ja resilienssin vahvistamisesta entistä tärkeämpää. Suomen ja Ruotsin Nato-jäsenyys jo aiemmin Natoon liittyneiden Norjan ja Tanskan vanavedessä mahdollistaa laajemman yhteistyön alueen infrastruktuurin ja digitaalisten palveluiden turvallisuuden ja resilienssin kehittämisessä.

Digitaalisten palveluiden tuottajien on Pohjoismaissa kehitettävä osaamistaan, palkattava henkilöstöä ja jaettava sekä ylläpidettävä teknisiä ratkaisuja yli rajojen suojatakseen viestintää, sisältöä ja kriittistä infrastruktuuria nopeasti muuttuvassa turvallisuusympäristössä. Tehokas vastaus näihin haasteisiin edellyttää yhtenäistä ja ennustettavaa sääntelyä sekä vahvempaa yhteistyötä Pohjoismaiden välillä digitaalisen infrastruktuurin, verkkojen häiriönsietokyvyn ja turvallisuuden lisäämiseksi. Nykyinen sääntely-ympäristö kuitenkin vaikeuttaa rajat ylittävää yhteistyötä.

Henkilöstöturvallisuuden varmistaminen on kriittistä verkkoturvallisuuden kannalta. Asianmukaiset turvallisuusselvitysprosessit ovat olennaisen tärkeitä henkilöstön luotettavuuden varmistamiseksi. Valitettavasti menettelyt vaativat tarkennusta lainsäädäntöön ja käytäntöihin, sillä nykyiset turvallisuusselvitysprosessit ja niiden kattavuus vaihtelevat Pohjoismaiden välillä. Tämä johtaa hankaliin, jopa käytännössä toimimattomiin, menettelyihin. Lisäksi maakohtainen lainsäädäntö on vaihtelevaa, kuten myös toimialakohtaiset vaatimukset.

Pohjoismaiden välisten turvallisuusselvitysprosessien yksinkertaistaminen ja yhdenmukaistaminen auttaisi tehostamaan kollektiivista turvallisuutta. Lisäksi se mahdollistaisi tiedon jakamisen ja digitaalisen infrastruktuurin häiriönsietokyvyn parantamisen. Tämä muutos helpottaisi yhteistyötä julkisella ja yksityisellä sektorilla ja tehostaisi verkkojen käyttöönottoa sekä mittakaavaetujen saavuttamista. Turvallisuusselvitysprosessien tulisi toimia yhdenmukaisesti ja yhtä nopeasti niin kansallisesti kuin Pohjoismaiden välillä.

Selkeänä toimenpiteenä tarvitaan pohjoismaista resilienssivähykettä julkisen ja yksityisen sektorin yhteistoiminnalle, tehostettua rajat ylittävää tiedonvaihtoa ja pitkäjänteisiä toimintamalleja kriittiseen infrastruktuuriin investoimiseksi. Pohjoismaisen yhteistyön tiivistäminen on välttämätöntä, jotta alueelle voidaan rakentaa strategisesti merkittävä kriisinsietokyky Euroopan turvallisuuden ja huoltovarmuuden näkökulmasta.

Kannatamme seuraavia toimenpiteitä:

1. Pohjoismaisen turvallisuusselvitysjärjestelmän kehittäminen: Luodaan koordinoitu pohjoismainen kehys henkilöstön turvallisuusselvityksille yhteisten periaatteiden mukaisesti. Tämä kehys virtaviivaistaisi rajat ylittävää selvitysprosessia ja mahdollistaisi tehokkaamman rajat ylittävän yhteistyön säilyttäen samalla korkeat turvallisuusvaatimukset.
2. Kansallisten autonomiavaatimusten arviointi: Tarkistetaan kansalliset autonomiavaatimukset rajat ylittävän yhteistyön mahdollistamiseksi. Tämä lähestymistapa helpottaa teknisten ratkaisujen ja infrastruktuurin jakamista keskeisillä maantieteellisillä alueilla, kuten Pohjoismaissa, ja parantaa turvallisuutta ja häiriönsietokykyä koko alueella.

3. Tehostetaan tiedon jakamista: Parannetaan uhka- ja turvallisuustietojen kaksisuuntaista jakamista julkisen ja yksityisen sektorin välillä sekä yksityisen sektorin tytäryhtiöiden välillä Pohjoismaissa. Tällä lähestymistavalla varmistetaan, että sekä keskeisillä puolustusalan toimijoilla että useilla Pohjoismaiden alueilla toimivilla yrityksillä on paremmat valmiudet vastata tehokkaasti muuttuviin uhkiin.

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

Suomen asema turvallisten ja luotettavien viestintäverkkojen edelläkävijänä perustuu innovatiiviseen, markkinaehtoiseen infrastruktuuriin ja edistykselliseen taajuuspolitiikkaan, joissa investointeja on edistetty nopean verkonrakentamisen mahdollistamiseksi taloudellisten tavoitteiden sijaan.

Jatkuvat parannukset takaavat verkkojen toimintavarmuuden myös häiriötilanteissa. Tulevaisuudessa Suomen menestyksen kulmakivinä ovat ennakoitava ja vakaa toimintaympäristö digikehitykselle, aktiivinen tutkimus- ja innovaatiotoiminta, digitaalisten taitojen jatkuva kehittäminen kaikilla koulutustasoilla sekä vahva rooli eurooppalaisen digipolitiikan muovaamisessa. Myös julkista rahaa tarvitaan investoinneissa sekä toimialarajojen yli tehtävää yhteistyötä.

Frosterus Heli
DNA Oyj