Puolustus- ja Ilmailuteollisuus PIA ry

Lausunto

29.08.2025

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?

Painotamme puolustuksen ja turvallisuuden näkökulmia alan teollisuuden toiminta- ja kilpailukyvyn kautta. Näemme nämä kaikkein keskeisimpinä kysymyksinä.

1.1 Teknologiset muutokset

Tarkasteltaessa teknologisia muutosajureita puolustuskontekstissa, voidaan yhtenä hyvänä ohjenuorana pitää NATO STO:n (Science and Technology Organization) julkaisemaa Science and Technology Trends 2025-2045 -dokumenttia. Suhteutettuna muihin vastaaviin koonnoksiin, kansalliseen ja kansainväliseen tutkimustoimintaan sekä viimeaikaiseen turvallisuuspoliittisen tilanteen pysyväisluontoiseen muutokseen, voidaan nimenomaan viestintäverkkoihin sidoksissa olevia teknologisia muutoksia arvioida ja ryhmittää tärkeimpiin kokonaisuuksiin. Seuraavassa tarkastellaan kutakin tunnistettua muutosajuria erikseen.

Teknologiakonvergenssi ja ohjelmistopohjaisuus

Yhtenä makrotrendinä teknologiassa on nähtävissä konvergenssi, jolla viitataan useiden, aiemmin yhtä tai vain tiettyjä toimintoja suorittavien erillislaitteiden yhdistyminen todellisiksi monitoimialustoiksi. Kun teknologian edelleen voimakkaana jatkuva miniatyrisoituminen sekä alati jatkuva ohjelmistopohjaisuuden lisääntyminen yhdistetään konvergenssitrendiin, nähdään jatkossa yhä enemmän aiempaa pienempiä, moneen asiaan samanaikaisesti kykeneviä laitteita ja järjestelmiä. Sotilasteknologiassa esimerkkinä voi olla vaikkapa kompakti järjestelmä, jossa samassa laitteessa yhdistyvät signaalitiedustelu, valvontaan ja tulenjohtoon kykenevä tutka, paikantamis- ja navigointilaite (PNT), häirintäjärjestelmä ja viestijärjestelmä. Käytettävän laitteiston fyysinen rakenne ja ominaisuudet asettavat toiminnalle mahdolliset rajoitteet, mutta varsinainen toiminto valitaan ja toteutetaan ohjelmistolla. Asiaa voidaan tarkastella myös toisinpäin: tällä hetkellä vallalla

oleva regulaatio ja lainsäädäntö eivät saa sanella ja rajoittaa esim. radiolaitteiden fyysisiä ja toiminnallisia ominaisuuksia (hardware), koska laitteista ulos saatava signaali tai muu toiminnallisuus toteutetaan ohjelmistollisesti. Regulaation muuttuessa ei tällöin tarvitse uusia koko kalustoa. Muistutamme, että liian tiukka regulaatio tappaa innovatiivisuuden.

Vaikka fysiikka tulee jatkossakin rajoittamaan teknologian käyttömahdollisuuksia (esim. antennien fyysisen koon riippuvuus käytettävästä aallonpituudesta), tulee järjestelmän osien toteutettavuus system-on-chip -periaatteella erillisille järjestelmäpiireille kiihdyttämään teknologian uusia käyttömahdollisuuksia (operatiivinen disruptio).

Toisena esimerkkinä konvergenssista on tulevaisuuden 6G-verkko ja siihen liittyvät langattomat teknologiat. 6G:n osalta aiempaa korkeampien taajuuksien käyttäminen (>100 GHz) kiihdyttää eri teknologioiden konvergoitumista entisestään. Esimerkiksi ympäristön havainnointi ja kuvantaminen sekä tarkka paikannuskyky yhdistettynä liikkuvaan viestintään ja koneoppimiseen luo täysin uusia teknologian käyttömahdollisuuksia. Vaikka tällä hetkellä visiot yhteiskunnallisesta kehittämisestä rakentuvatkin paljolti mm. 6G-teknologian mahdollistamaan ubiikkiin eli jatkuvasti läsnä olevaan internettiin ja liitettävyyteen ja sitä kautta ihmiskunnan hyvinvointia lisääviin sovelluksiin ja palveluihin, pitäisi samalla osata arvioida myös kansakuntaamme kohdistuvia uhkia ja niiden torjuntaan liittyviä mahdollisuuksia. Vastaavasti hyvin toimivaa verkkorakennetta voidaan käyttää puolustajan kannalta hyödyksi esimerkiksi maahan tunkeutuvien joukkojen ja järjestelmien tunnistamisessa, seurannassa ja niihin vaikuttamisessa.

Sähkömagneettisen spektrin hallinta

Sähkömagneettisen spektrin käyttöön liittyvä jäykkä lainsäädäntö voi pahimmillaan rajoittaa uusien innovaatioiden synnyttämistä. Jo yksistään 6G-teknologian siirtyminen korkeammille taajuuksille tuo mukanaan uusia teknologian käyttömahdollisuuksia, puhumattakaan edellä käsitellyn teknologiakonvergenssin suomista mahdollisuuksista.

Sähkömagneettinen spektri tunnetaan kolmesta c:stä: congested, contested, constrained. Tällä viitataan siihen, että jo nyt spektri on erittäin ruuhkainen, sen käytöstä pyritään kilpailemaan voimakkaasti, ja että sen käyttöä pyritään reguloimaan vahvasti. Spektrin käytöstä itsensä riippuvaiseksi tekevä tietoyhteiskunta joutuu väkisinkin rakentamaan resilienssiä toiminnoilleen selvitäkseen jatkossakin varmasti esiintyvistä häiriötekijöistä (luonnonmullistukset, sähkökatkokset, rikollinen toiminta, sota jne.).

Hyvin vähän julkisuudessa käsitelty näkökulma liittyy puolustukseen: millä tavalla yhteiskunta aikoo varautua NATO:n toteuttamiin operaatioihin Suomen tai koko Pohjolan alueella? Millä tavalla spektriä hallitaan ja kenen toimesta silloin, kun pahimmassa tapauksessa maan alueella on käynnissä sotilasoperaatio, ja kun yhteiskunnan perustoiminnot tuketuvat enenevässä määrin spektrin

käyttöön? Suuren sotilasjoukon tarvitsema emittereiden ja häirintälaitteiden määrä moninkertaistaa Suomen alueella toteutettavan tietoliikenteen ja sensorien määrän. On myös oletettavaa, että vastustaja ei kunnioita kansainvälisiä taajuusallokaatioita ja muita spektrin käyttöön liittyviä määräyksiä. Koska sähkömagneettinen signaali ei tunne rajoja, ei sitä koskeva lainsäädäntö voi vaihdella maasta toiseen – kuten tällä hetkellä on tilanne esim. Pohjoismaiden välillä. Suomi ja Pohjoismaat tarvitsevat 2030-luvulla:

- Dynaamista ja mielellään kognitiivista spektrinhallintaa.
- Harmonisoitua lainsäädäntöä sähkömagneettisen spektrin osalta.

On huomattava, että sotilaallisesta sisällöstään huolimatta edelliset kohdat koskevat mitä suurimmassa määrin myös siviiliyhteiskuntaa: millä tavalla keskeisimmät toimintonsa (energiantuotto ja jakelu, vesihuolto, matkapuhelinverkot, liikenne, pankki- ja vakuutuslaitokset, rahaliikenne jne.) sähkömagneettisesta spektristä riippuvaiseksi tehnyt tietoyhteiskunta hallitsee ja sovittaa yhteen alueen sotilastoimijat ja siviiliyhteiskunnan toiminnot vakavissa häiriötilanteissa?

6G-verkko ja uudet langattomat teknologiat

Uusi verkkosukupolvi syntyy tunnetusti n. 10 vuoden välein. Siten tulevan 6G-verkon voidaan olettaa olevan käytössä 2030-luvun puolivälissä. Suomi on profiloitunut luunkovana tietoliikenne- ja verkkoteknologian osaajana ja näin tulee olla jatkossakin. Tässä mielessä 6G-teknologiaa pitää kyetä tarkastelemaan myös puolustuksen ja turvallisuuden näkökulmista (ks. em. konvergenssi-kohta). Puolustusteollisuus on nousussa vielä useita vuosia pitkälle 2030-luvulle, jolloin 6G-teknologian oletetaan olevan jo käytössä. Puolustusteollisuuden tulee näkyä myös kansallisissa hankkeissa hyväksyttävänä toimialana.

Avaruusteknologia

Avaruuden merkitys yhtenä sodankäynnin operaatioympäristönä on jatkuvassa nousussa. Toisaalta myös siviiliyhteiskunnan monet toiminnot hyödyntävät avaruutta enenevässä määrin. Suomen kaltaisen syrjäisen ja pohjoisen maan tulee rakentaa sekä omia että yhteisiä kykyjä avaruuteen kumppanimaiden kanssa. Satelliittitietoliikenne ja sensoritiedon välittäminen (sotilastiedustelu, kaukokartoitus, sään seuranta, navigointi, paikkatieto ja aikareferenssi jne.) vaativat laajakaistaisia ja samalla tietoturvallisia viestintäratkaisuja, jotka eivät ole alttiita häirinnälle ja häiriöille. Suomalainen avaruusteollisuus on yksi teknologisesti kehittyneimmistä ja liiketoiminnan laajuudella mitattuna suurimpien joukossa Euroopassa. Suomen tuleekin tukea EU:n ns. flagship-projektien toteutusta

voimakkaasti ja huolehtia siitä, että kotimaisella avaruusteollisuudella on tasaveroiset edellytykset osallistua näihin projekteihin.

Avaruuden merkityksen kasvaessa ja toisaalta sinne pääsyn helpottumisen myötä ei enää voida tuudittautua pelkästään sen rauhanomaiseen käyttöön. Avaruudessa käytettävien järjestelmien ja aaltomuotojen tulee varautua häirintään, harhautukseen, satelliittien tuhoamisjärjestelmiin, avaruuden ruuhkautumiseen ja avaruusroskan lisääntymiseen, kyberhyökkäyksiin ja suunnatun energian aseisiin (DEW, Directed Energy Weapons). Kaikkia edellä mainittuja keinoja tullaan käyttämään myös siviilikäyttöön ensisijaisesti tarkoitettuja satelliitteja vastaan, jos ja kun niistä nähdään olevan myös sotilaallista hyötyä.

Elektroninen sodankäynti

Elektroninen sodankäynti (ELSO) on ns. ei-kineettinen sodankäynnin muoto, jossa vastustajan sensori-, tietoliikenne ja asejärjestelmiä tiedustellaan, tai niihin vaikutetaan sähkömagneettisen spektrin kautta. ELSO:sta on Ukrainan sodan myötä kirjoitettu verraten paljon etenkin droonisodankäynnin yhteydessä. ELSO on joka tapauksessa käyttökohteiltaan huomattavasti laajempi kokonaisuus kuin pelkkä vastadroonimekanismi.

Koska yhteiskunnan riippuvuus spektristä kasvaa entisestään, ja koska moni viestintään tai viestintäverkkoon tietoa tuottava järjestelmä perustuu ns. kaksikäyttötuotteisiin, on jatkossa entistä vaikeampaa tehdä suoraa jakoa näiden järjestelmien osalta puhtaasti puolustus- tai siviilituotteisiin. Tässä mielessä myös siviiliyhteiskunnan viestintäverkot tulisi rakentaa kestämään elektronisen sodankäynnin eri ilmenemismuotoja. Toisin sanoen verkkojen tiedusteltavuus tulisi minimoida esimerkiksi hajasäteilyn osalta, aaltomuotojen tulisi olla häirintää sietäviä (teho, taajuus, hajaspektritekniikat jne.), kryptoalgoritmien tulisi olla riittävän vahvoja, tulevaisuudessa esim. kvanttiteknologiaa tulisi hyödyntää tekniikan sallimissa mitoissa jne. Julkisissa hankinnoissa ja samoin myös kriittisten toimijoiden tuottamissa viestintäverkkopalveluissa elektronisen sodankäynnin asettamat vaatimukset tulisi osata asettaa ja arvioida. Viestintäverkkojen ja niihin liittyvien palveluiden edes osittainen lamauttaminen ei saa kaataa tulevaisuuden tietoyhteiskuntaa. Tästä johtopäätöksenä on se, että siviiliyhteiskunnan tulee varautua myös teknisessä mielessä sotilaallisiin uhkiin resilienssin kasvattamiseksi.

Kybersuojaus

Järjestelmien ja viestintäverkkojen kybersuojauksen merkitys ja taso tuskin tulee vähenemään seuraavan vuosikymmenen aikana. Organisaatioiden tulee kyetä rakentamaan tuottamansa järjestelmät ja palvelut mahdollisimman kybervarmoiksi, mutta kuitenkin käyttökelpoisiksi tuotteiksi. Viime kädessä kansallisen kyberturvallisuuskeskuksen (vast.) pitää kyetä toimimaan yhteiskunnan kriittisten toimijoiden suojana.

Vahvennetun kybersuojauksen tarpeen ajureina voivat olla mm. etätyön ja erilaisten pilvipalveluiden yleistyminen ja ylipäätään hajautettu työskentely- tai toimintamalli. Zero Trust -arkkitehtuurin lisääntyminen organisaatioissa on hyvä esimerkki suojautumiseen varautumisesta – tämän toimintamallin merkitys korostunee myös kymmenen vuoden tarkastelujaksolla. Ennen kaikkea tekoäly voi tuoda tähän tietoturvamalliin uusia vahvistavia elementtejä.

Kvanttiteknologia

Työ- ja elinkeinoministeriö on julkaissut varsin kunnianhimoisen kvanttiteknologiastrategian 2025-2035. Sen mukaan Suomeen halutaan maailman kärkiluokan kvanttilaskentaympäristö, kvanttilaitteiden kehitystä tukeva infrastruktuuri, osaamisen vahvistaminen, pitkäjänteinen TKI-ohjelma, yritysten globaalin kasvun rahoitus sekä kansainvälinen yhteistyö.

Vaikka kvanttilaskentaan liittyykin vielä suuria epävarmuuksia, ovat tieteenalaan liittyvät odotukset suuria. Kvanttilaskennalta odotetaan mm. monituhatkertaista laskentakapasiteettia nykyisiin supertietokoneisiin verrattuna. Lisäksi salaustekniikoihin odotetaan merkittäviä parannuskeinoja esim. kvanttiturvallisten salausmenetelmien (Post Quantum Cryptography, PQC) ja kvanttiavainten jakoon liittyvillä teknologioilla (Quantum Key Distribution, QKD). Näillä menettelyillä uumoillaan saavutettavan teoriassa murtamaton salaus, jossa myös kvanttilinkin salakuuntelu havaittaisiin välittömästi. Lisäksi kvanttiteknologialla oletetaan saatavan aikaan erittäin tarkka paikannus ja aikareferenssi ilman satelliittipohjaisia järjestelmiä.

Suomessa on korkeatasoista kvanttialan osaamista sekä yrityksissä että tutkimusyhteisössä; lisäksi tutkimustoimintaa ja uusien tuotteiden kehittämistä tuetaan strategian mukaisesti tutkimus- ja innovaatiorahoituksella. Suomella on siten hyvät lähtökohdat profiloitua kvanttiteknologian kärkimaaksi. Onnistuessaan kvanttiteknologia voi mullistaa nykyisen viestintäverkkoinfrastruktuurin, joskaan tämän varaan ei kannata sokeasti luottaa. On kuitenkin todennäköistä, että alan kehitystä tulee tukea ja seurata erityisen tarkasti samalla, kun toimivaksi osoitettuja innovaatioita otetaan ennakkoluulottomasti käyttöön lähestyttäessä 2030-lukua.

Tekoäly ja koneoppiminen

Tekoälyä on vaikeaa tarkastella erillisenä kokonaisuutena, joka ikään kuin ”liimataan” vaikkapa verkkosuunnittelun tai tietoliikennejärjestelmän päälle. Tekoälypohjaiset ratkaisut on osattava ottaa huomioon mm. verkko- ja järjestelmäsuunnittelussa alusta lähtien niiden luonnollisena osana.

Suomi julkaisi oman tekoälystrategiansa jo v. 2017 ja osoitti tuolloin olevansa alan kärkimaita. Sittemmin Suomen sijoitus kansainvälisissä vertailuissa on pudonnut johtuen paljolti yrityskentän varovaisuudesta ja investointihalukkuuden pienuudesta. Kansallista tekoälystrategiaa päivitetään parhaillaan, minkä toivotaan ohjaavan maan tekoälykehitystä kohti Euroopan kärkeä panostamalla mm. tekoälyn turvalliseen ja vastuulliseen käyttöön.

Usein tekoälyn yhteydessä puhutaan myös koneoppimisesta. Tekoälyä voidaan pitää laajana yläkäsitteenä teknologioille, jotka jollakin tavalla pyrkivät jäljittelemään ihmisen älykkyyttä. Koneoppimista voidaan pitää tekoälyn osa-alueena, jossa sitä hyväksikäyttävät järjestelmät oppivat käytössään olevasta datasta halutun toimintamallin ilman erillistä ohjelmointia. Syväoppimisesta (Deep Learning) voidaan puhua silloin, kun koneoppiva järjestelmä käyttää monikerroksisia neuroverkkoja datan automaattiseen analysoimiseen. Sovelluskohteita voivat olla mm. kuvan- ja puheentunnistus ja kielen käsittely.

Tekoäly ja koneoppiminen vaikuttavat 2030-luvun viestintäverkkoihin jo aivan ylätason toimintamallien kautta. Esimerkiksi verkkosuunnittelu ja verkkojen ylläpito saattavat muuttua konseptuaalisesti täysin erityyppisiksi kuin nykypäivänä. Erityisen mielenkiintoista voisi olla langattomien verkkojen osalta tekoälypohjainen kognitiivinen spektrinhallinta, jolla kulloinkin tiettyyn aikaan kyseisellä alueella vapaana olevat viestintäkanavat olisivat aina löydettävissä automaattisesti. Rajoittavana tekijänä monessa suhteessa voi olla kansallinen ja kansainvälinen regulaatio.

1.2 Taloudelliset muutokset

Huolimatta puolustuksen tarpeiden merkittävästä kasvusta, Suomen kyetä edelleen tekemään joustavaa ja rahoitustasoltaan riittävää tutkimus-, kehitys- ja innovaatiopolitiikkaa. Esimerkiksi edellä esitetyt kvanttiteknologian ja tekoälyn strategiat eivät toteudu, jos julkishallinto ei kykene panostamaan uuden teknologian tutkimukseen ja käyttöönottoon vaaditulla tasolla. Julkishallinnon tulee kyetä tarjoamaan yrityselämälle houkuttelevia kannustimia, kuten tulevia hankkeita, esim. 6G-teknologian ja tekoälyn laajaan hyödyntämiseen. Samalla tulee aktiivisesti tiedottaa ja kannustaa tavallisia kansalaisia uuden teknologian käyttöönottoon.

Kuituverkkojen ja ennen kaikkea 6G-verkon rakentaminen vaatii merkittäviä julkisia ja yksityisiä investointeja. Etenkin yrityksiä tulisi rohkaista nykyistä laajempaan riskinottoon ja toiminnan kääntämiseen kasvu-uralle säästökohteiden hakemisen sijaan.

1.3 Geopoliittiset muutokset

Venäjä ja sen luoma uuteen maailmanjärjestykseen pyrkivä ekspansiivinen politiikka tulee vaikuttamaan Suomeen, eikä vaikutus rajoitu pelkästään ulko- ja turvallisuuspolitiikkaan, sillä Venäjän hybridisodankäynnin eri muotoihin on varauduttava myös siviiliyhteiskunnassa kaikin tavoin. Viestintäverkkojen osalta tämä tarkoittaa aiemmin sotilasteknologiaan liitettyjen suojautumiskeinojen soveltamista siviiliteknologiaan, verkkotopologioihin jne. Kuten aiemmin luvussa 3.1 on tuotu esille, siviili- ja sotilasteknologia tulevat konvergenssin, ohjelmistopohjaisuuden ja kaksikäyttöisyyden myötä lähentymään toisiaan, usein jopa siinä määrin, että niitä ei välttämättä ole enää toiminnallisesti järkevää erotella toisistaan. Koska turvallisuusuhka koskee nykykokemusten mukaan selkeästi koko yhteiskuntaa, pitää yhteiskunnan resilienssiä kyetä rakentamaan sekä toiminnallisin että teknologisin keinoin. Yksinkertaistettuna tämä tarkoittaa sitä, että ainakin julkisilla varoilla rakennettavassa teknologiassa on otettava huomioon kybersuojautuminen ja elektronisen sodankäynnin vaikutukset, puhumattakaan fyysisestä suojautumisesta ja verkkojen redundanttisuudesta.

Koska Suomi ei toimi muusta maailmasta eristettynä saarekkeena, pitää kansainvälisten tietoliikenneyhteyksien toiminta turvata redundanttisuudella, kansainvälisillä sopimuksilla ja riittävällä valvonnalla.

Huoltovarmuuden osalta pitää pyrkiä lyhentämään tilaus-toimitusketjuja ja varaamaan maahan riittävä määrä kompetenssia ja varaositusta järjestelmien ylläpitoon. Tässä suhteessa ei aina kyetä tukeutumaan kansainvälisiin huoltosopimuksiin, koska tunnetusti syvän kriisin aikana materiaalin lähettäminen ulkomaille korjattavaksi ei aina ole mahdollista. Tässä mielessä Just-In-Time -ajattelu ei enää päde 2030-luvun Suomessa.

EU-tasolla tarkasteltuna tulisi kyetä luomaan Eurooppaan kriittisiä kyvykkyyksiä niin osaamisen kuin itse tuotteiden valmistuksenkin osalta. Tätä kehitystä on syytä tukea sekä talouselämän että julkishallinnon puolelta.

Itärajan läheisyys tulee aina vaikuttamaan Suomen ajattelumalleihin ja toiminnallisiin ratkaisuihin. Lähtökohtana tulee kuitenkin olla viestintäverkkojen toimivuus koko maassa.

1.4 Yhteiskunnalliset muutokset

Suomen talouselämä ja julkisyhteisö tarvitsevat osaavaa henkilöstöä. Koulutuksen muovaaminen työelämän tarpeita vastaavaksi on keskeistä. On ennakoitavissa, että tekoälyn käytön laajentuminen tulee vapauttamaan merkittävän määrän työvoimaa markkinoille seuraavan kymmenen vuoden aikana. Tämän työvoimareservin uudelleen kouluttamiseen tulee varautua ennakoivasti jo nyt.

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

Venäjän muodostamaa uhkaa yhtäältä Suomelle ja toisaalta koko Euroopalle ei sovi unohtaa. Vaikuttaa kuitenkin siltä, että joitakin siviiliyhteiskunnan sovelluksia rakennetaan lähinnä kestävä kehitys edellä, samalla unohtaen riittävälle tasolle ulottuvat puolustuksen, turvallisuuden ja yhteiskunnan resilienssin tarpeet.

Pitkällä aikavälillä tarkasteltuna voitaisiin saada aikaan kansantaloudellisesti säästöjä rakentamalla siviilikäyttöön tarkoitettuihin viestintäverkkoihin ja laitteistoihin jo lähtökohtaisesti sotilaallisia ominaisuuksia. Vastaavasti sotilasteknologiassa tulisi harkita entistä laajempaa tukeutumista siviili-infrastruktuuriin. Verkottamalla tulevaisuuden tietoyhteiskunta keskeisimmiltä ominaisuuksiltaan toisiinsa, voidaan yhteiskunnan kokonaisresilienssiä parantaa nykyisestä. Entistä parempiin kansainvälisiin asemiin ja verkostoihin pääsevällä puolustusteollisuudella voisi olla paljon annettavaa tässä kokonaisuudessa.

Suomalaisen teollisuuden roolia kokonaisturvallisuuden ja resilienssin tuottajana ei sovi unohtaa. Kun tilaus-toimitusketjut ovat sopivan lyhyitä, on hädän tullen apukin lähellä. Kansainvälisten sopimusten voimaan ei voi liiaksi luottaa, kuten näimme mm. pandemian aikana. Hankintalakia tulkitaan usein liian ahtaasti. Vertailukriteereinä tulisi laajemmin käyttää kokonaistaloudellista edullisuutta, jonka perusteisiin voidaan sisällyttää esim. huoltovarmuuden elementtejä.

Onpa sitten kyse viestintäverkkoihin liittyvästä kokonaisuudesta tai laajemmasta viitekehyksestä, pitäisi Suomen tutkimus- ja käyttäjäyhteisön olla tiiviisti mukana sekä EU-vetoisen että kansallisen regulaation laadinnassa. EU:n ei saa antaa jäädä takamatkalle tappamalla innovaatiopotentiaali jäykän ja monelta osin myös asenteellisen regulaation vuoksi. Edellä on kuvattu esimerkkejä sähkömagneettiseen spektriin liittyvästä regulaatiosta, joka on jossain määrin jäänyt teknologiakehityksen jalkoihin. Sama asia tulee eteen tekoälyn, kybersuojauksen ja vastaavien teknologia-alueiden kanssa.

Kiteytettynä viestintäinfrastruktuuriin liittyvät erityistarkasteltavat teemat voisivat sisältää ainakin seuraavat asiat:

- Puolustuksen ja turvallisuuden erityisvaatimukset viestintäinfrastruktuurille yhteiskunnan kokonaisturvallisuuden osana.
- Kotimainen ja eurooppalainen huoltovarmuus
- Kotimainen ja eurooppalainen regulaatio ja lainsäädäntö

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?

Digitalisaatioon liittyvä taloudellinen potentiaali pitää osata ulosmitata mahdollisimman monia hyödyttävällä tavalla, mutta kuitenkin turvallisesti. Maassamme on tälläkin hetkellä lukuisia esimerkkejä siitä, kuinka avoimeen dataan perustuvaa informaatiota on voinut miltei kuka vaan verkkoon pääsevä henkilö tutkia ja jopa ladata itselleen oikeaa käyttötarkoitusta määrittelemättä. Vaikka avoimen yhteiskunnan periaate on hyvä, pitää sekä julkishallinnon että yrityselämän ottaa pahansuopa käyttötarkoitus huomioon erilaisia ratkaisuja suunniteltaessa. Kriittisten viestintäverkkojen kuvaus (fyysinen ulottuvuus, kryptaus, haavoittuvuudet jne.) on osattava pitää salassa ja valtuutettujen toimijoiden tiedossa.

Suhtautuminen tietoturvaan ja turvallisuusuhkiin ei ole samalla tasolla eri organisaatioissa ja maissa. Nämä uhat on kyettävä tunnistamaan riittävän ajoissa vahinkojen estämiseksi.

Tiedon eheyden osalta Suomessa on paljon tehtävää. Tekoälyn avulla tuotettavan disinformaation määrä on nyt ja jatkossa valtava, ja juuri tällä pyritään vaikuttamaan kansakuntien, organisaatioiden ja jopa yksittäisten kansalaisten mielipiteisiin. Kansalaisten luottamus on voitava ansaita, mutta toisaalta kansalaisia on kyettävä kouluttamaan hybridivaikuttamisen tunnistamisessa. Epäluottamus datan käyttöön voi hidastaa uusien palveluiden käyttöönottoa.

Yhteiskunnan on luotava yrittäjämyönteinen ilmapiiri investointien tukemiseksi esimerkiksi pienyritysten ja start-upien rahoitushaasteiden taklaamiseksi. Massiiviset investoinnit esim. datakeskuksiin vaativat ennakoivaa sääntelyä ja julkisen sektorin tukea.

Osaajapulaan ja työvoiman kohtaanto-ongelmaan otettiin jo aiemmin kantaa tässä lausunnossa. Asiaa ei sovi unohtaa, sillä tämä on erittäin suuri kasvun ja investointien este.

Riippuvuus Euroopan ulkopuolisesta teknologiasta on erittäin suuri riski suomalaisen tietoyhteiskunnan – samalla myös viestintäinfrastruktuurin – näkökulmasta. Tietoliikenteessä ja viestinnässä käytetyt laitteet ja ohjelmistot voivat jo sinänsä muodostaa tietoturvariskin, puhumattakaan suurten alustatoimijoiden hallitsevasta ja kilpailua vääristävästä markkina-asemasta. Huoltovarmuuden kannalta kotimainen ja eurooppalainen teknologia olisi paras lähtökohta.

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

NATO-jäsenyys on sinetöinyt Suomen erittäin vahvasti läntiseen viitekehykseen turvallisuuden tuottajana. Tämä seikka heijastuu koko yhteiskuntaan sekä siihen, miten Suomeen suhtaudutaan.

Suomalaisiin, suomalaiseen teknologiaan ja yhteiskuntaan luotetaan. Suomen kokonaisturvallisuuden toimintamallia arvostetaan ja ihmetellään – tämä on meille kansainvälinen myyntivaltti, mikä pitää säilyttää ja vahvistaa.

Suomen tulee kyetä osata valita ne teknologiset keihäänkärjet, joissa haluamme profiloitua maailmanluokan osaajiksi. 1990-luvulla yksi näistä oli tietoliikenne ja tietoliikenne sekä informaatioteknologia laajemminkin voisivat olla uuden ajan vetojuhtina. Teknologiakonvergenssin myötä Suomessa on maailmanluokan osaamista mm. tekoälyssä, kryptologiassa, kyber- ja kvanttiteknologiassa sekä langattomassa tiedonsiirrossa. Kaikki edellä mainitut liittyvät viestintäverkkoihin ja niitä tukevaan kokonaisuuteen. Lisäksi meillä on lukuisa joukko epäsuorasti tietoliikennettä ja viestintäverkkoja tukevia teknologian osaamisalueita; esimerkkinä mainittakoon lisätyn todellisuuden teknologiat (AR/VR/XR). Suomalaisen innovatiivisuuden mittarina voidaan pitää kykyä integroida erilaisia teknologioita out-of-the-box -tyylisesti toimiviksi järjestelmiksi ja kansainvälisiksi myyntivalteiksi.

Tässä lopussa esitetään ilman kattavia perusteluita luettelomaisesti seikkoja, joilla koemme olevan keskeinen rooli Suomen houkuttelevuuden ja edistyksellisyyden lisäämiseksi turvallisten ja luotettavien viestintäverkkojen ja -teknologioiden käytössä.

- Sääntöperusteisen yhteiskunnan vahvistaminen:
  - Huolehditaan siitä, että kansallinen lainsäädäntö ja regulaatio ovat riittävän vahvoja ja määrätietoisia, mutta samalla kuitenkin riittävän sallivia innovaatiokyvyn edistämiseksi.
  - Osallistutaan vahvalla panoksella EU-regulaation suuntaamiseksi nykyistä sallivampaan ja innovaatiotoimintaa tukevampaan suuntaan.
- Kansallinen kokonaisturvallisuuden toimintamalli:
  - Markkinoidaan maamme ainutlaatuista kokonaisturvallisuusmallia vientiponnistelujemme tukena.
  - Koordinoidaan tehokkaasti eri hallinnonalojen laatimat teknologioihin ja talouskasvuun liittyvät kansallisen tason strategiat ja niiden toimeenpano.
  - Huolehditaan eri viranomaisten toimivaltuuksien saumattomasta koordinaatiosta.
  - Osallistutaan proaktiivisesti ja uskottavalla sekä näkyvällä tavalla NATO:n ja EU:n toimintaan.
- Teknologisena suunnannäyttäjänä toimiminen:
  - Panostetaan 2030-luvun kärkiteknologioihin strategialinjausten mukaisesti.
  - Luodaan yhteiskuntaan ennakkoluuloton ja kokeileva, innovaatioita tukeva ilmapiiri niin julkishallinnossa, tutkimusyhteisössä kuin yrityselämässäkin.

o Vahvistetaan uskottavalla ja näkyvällä tavalla Euroopan teollista suvereniteettia riippumattomien teknologisten tutkimus-, innovointi-, kehitys- ja tuotantokykyjen luomisella Suomeen.

o Luodaan itsellemme etulyöntiasema langattomien verkkojen rakentamisessa ja hyödyntämisessä sekä niihin liittyvän teknologian suunnittelussa ja tuotannossa.

o Varmistetaan omalta osaltamme kansallisen ja EU-tasoisen tutkimus- ja innovaatiopolitiikan jatkumo sekä kansallisissa budjeteissa että EU:n pitkän aikavälin rahoitussuunnitelmissa (Multiannual Financial Framework, MFF).

 Osaava työvoima ja valistunut kansakunta

o Tehdään tietoturvallisesta viestinnästä kansalaistaito

o Vahvistetaan maamme osaamispohjaa ja huolehditaan sitä tukevasta koulutuspolitiikasta. Huolehditaan yritysten, tutkimuslaitosten ja julkishallinnon kyvystä palkata nuoria osaajia harjoittelupaikkoihin ja valmistumisen jälkeisiin töihin.

Karanko Tuija
Puolustus- ja Ilmailuteollisuus PIA ry