

FiComin lausunto tulevaisuusselonteosta

VNS 16/2022 vp Valtioneuvoston tulevaisuusselonteon 1. ja 2. osa: Näkymiä seuraavien sukupolvien Suomeen

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt FiComilta lausuntoa **Valtioneuvoston tulevaisuusselonteon 1. ja 2. osa: Näkymiä seuraavien sukupolvien Suomeen**. FiCom kiinnittää lausunnossaan huomiota Suomen tulevaisuuteen vaikuttaviin teknologisiin muutostekijöihin: kyberturvallisuuteen, avaruuden strategiseen merkitykseen, energiamurrokseen ja kriittiseen infrastruktuuriin.

FiComin keskeiset viestit

- Suomen vahvuutena on yksityisen ja julkisen sektorin luottamuksellinen yhteistyö. Viranomaisten rooli on koordinoida asioita eri hallinnonalojen välillä ja luoda yhteinen kuva kyberturvallisuuden tilanteesta. Yrityksillä taas on kyky suojata tietojärjestelmiä ja -infraa kyberhäiriöiltä ja -hyökkäyksiltä.
- Avaruuden strateginen merkitys huomioitava myös satelliittilaajakaistan ottamisesta mukaan yleispalveluyrityksen nimeämistä koskevassa arvioinnissa. Kyseessä on toimintavarma tekniikka ja Starlink on globaali vakavarainen ja liikevaihdoltaan merkittävä palveluntarjoaja, joka tarjoaa jo tällä hetkellä palveluitaan useassa kymmenessä maassa.
- ICT-alalla on iso kädenjälki energiansäästöä ja energiatehokkuutta toteutettaessa. Tietoliikennealan tarjoamat tuotteet ja palvelut auttavat kuluttajia ja muita toimialoja parantamaan omaa energiatehokkuuttaan mm. liikenteessä, teollisuudessa, rakentamisessa ja etätyössä.
- Keskeiset kriittiset infrakohteet ovat houkuttelevia iskukohteita kriisitilanteissa. Merikaapeleiden erittäin tarkat paikkatiedot avoimena netissä ja valtion hanke kerätä kaikki kriittinen infratieto yhteen valtiolliseen datapankkiin on arvioitava uudelleen.

Kyberturvallisuuden merkityksen korostuminen

Selonteossa todetaan, että tarve ymmärtää kyberturvallisuuden merkitys kaikilla tasoilla on voimakkaasti kasvanut. Keskusjohtoisuus ei ratkaise kaikkea, vaan yritysten toimintaedellytyksiä tulee parantaa. Olennaista on myös tukea yksilön, yhteisöjen ja yritysten valmiuksia ymmärtää muuttuvia tiedon ja turvallisuuden kysymyksiä.

On erittäin hyvä, että selontekokin selkeästi tuo esiin kyberturvasta huolehtimisen olevan ennenkaikkea yritysten varautumisen varassa. Yhteiskunta asettaa yhteiset raamit toiminnalle.

Viestintäverkkojen turvallisuus- ja varautumissääntelyllä on Suomessa pitkät perinteet. Se on myös hyvin kattavaa: pelkästään sähköisen viestinnän palvelulaissa (SVPL) on kokonaiset omat lukunsa – noin kaksikymmentä pykälää ja niiden alla useita momentteja – jotka liittyvät verkkojen tietoturvaan.

Myös kansallinen turvallisuus on SVPL:ssä huomioitu monessa kohdassa. Siinä esimerkiksi määritellään, millä edellytyksillä matkaviestinverkkojen toimilupia ja radiolupia voidaan myöntää. Lisäksi julkisen hallinnon turvallisuusverkkotoiminnasta on oma lakinsa, jolla on liittymäkohtia myös sähköisen viestinnän palvelulakiin.

Vain kaksi vuotta sitten uudistettuun sähköisen viestinnän palvelulakiin säädettiin uusi pykälä, joka koskee viestintäverkon kriittisissä osissa käytettäviä laitteita. Lisäksi Liikenne- ja viestintävirasto Traficom antoi asiaa koskevan määräyksen. Sääntelyä valmisteltiin laajassa yhteistyössä viranomaisten ja teleoperaattorien kanssa.

Verkkojen kriittisten osien sääntely koskee sekä kiinteää että mobiiliverkkoa, mutta sen pääpaino on mobiiliverkoissa, etenkin 5G-verkon kriittisissä osissa. Säännös ja sitä koskeva määräys ovat dynaamisia ja hyvin aikaa kestäviä. Niissä on huomioitu pragmaattisella ja yhteensovitetulla tavalla sekä kansallinen että verkkojen turvallisuus, verkkotekniikka ja toimintaympäristö palveluiden jatkuvuuden kannalta.

Traficom on lisäksi antanut SVPL:n nojalla puolenkymmentä määräystä ja suositusta viestintäverkkojen tietoturvasta. Nämä muodostavat säädöskehikon, joka teleyrityksen on otettava huomioon suunnitellessaan, rakentaessaan ja ylläpitäessään verkkoja. Yksi suomalainen erikoispiirre on viestintäverkkojen varmistamista koskeva määräys, joka esimerkiksi velvoittaa teleyrityksiä huolehtimaan tukiasemien sähkönsyötöstä akustojen tai generaattoreiden avulla sähkökatkosten aikana. Määräys osoittaa konkreettisella tasolla varautumissääntelyn pitkät perinteet, ja näinä aikoina varautumista koskeva määräys lienee ajankohtaisempi kuin koskaan.

Osana kansallista turvallisuutta ovat siviili- ja sotilastiedustelua koskevat säännökset. Tiedustelusääntely on toimivaa ja osoittanut tarpeellisuutensa. Se mahdollistaa valikoidun tiedustelutiedon jakamisen myös teleyrityksille. Tiedustelulaissa on kuitenkin joitain valuvikoja tietoturvallisuuden sekä viestintäverkkojen ja -palveluiden toimivuuden kannalta. Tällaisia ovat muun muassa viranomaisten oikeus asettaa omia laitteitaan tai ohjelmistojaan teleyrityksen verkkoihin näiden tietämättä. Tämä on huomattava uhka palveluiden häiriöttömyydelle ja tietoturvallisuudelle. Verkkojen turvallisuus ei saa vaarantua missään tilanteissa.

Suomessa viestintäverkkojen tietoturvasääntely on lähtökohtaisesti kunnossa, eikä lisäsääntelylle ole suurempia tarpeita. Pelkkä sääntely ja velvoitteiden täytäntöönpano ei kuitenkaan riitä – tarvitaan myös kaikkien alan toimijoiden yhteistyötä.

Teleyrityksillä on vahvaksi muodostunut luottamus Traficomin Kyberturvallisuuskeskuksen asiantuntevaan toimintaan, ja yhteistyö Kyberturvallisuuskeskuksen kanssa on tiivistä ja jatkuvaa. On hienoa, että valtion talousarvioissa vuodelle 2023 osoitettiin Kyberturvallisuuskeskukselle lisärahoitusta.

Kybervarautumisen ytimenä tulee jatkossakin olla yksityisen ja julkisen sektorin yhteistyön vahvistaminen. Yritysten tulee kertoa myös heikot signaalit ja havainnot viranomaisille, mutta tiedon pitää kulkea molempiin suuntiin mutkattomasti. Mitä varhaisemmassa vaiheessa yrityksillä on tieto mahdollisista uhkista, sitä vahvemmin ne pystyvät niihin varautumaan.

Avaruuden strateginen merkitys kasvaa

Selonteossa todetaan, että avaruustoiminnalla on yhä suurempi merkitys yhteiskunnan toimivuudelle, sisäiselle ja kansalliselle turvallisuudelle ja eri hallinnonalojen päätöksenteolle. Useat toimialat hyödyntävät satelliittien tuottamaa ja välittämää dataa. Esimerkiksi 5G-tietoliikennetarkaisut ja sään ennustaminen ovat riippuvaisia satelliittien tarjoamasta infrasta. Myös useat liikenteen, teollisuustuotannon sekä maa- ja metsätalouden palvelut tukeutuvat satelliittien tarjoamiin ratkaisuihin.

Valtioneuvoston selonteossa Suomen digitaalisesta kompassistakin todetaan, että satelliittilaajakaistan kehittämisen keskeisenä ajurina on varmistaa yhteyksien saatavuus kaikissa tilanteissa ja parantaa alueellista kattavuutta (VNS 10/2022 vp s. 48). Kirjaus satelliittilaajakaistan tarpeesta on hyvin selkeä. Se soveltuu nimenomaan erinomaisesti yleispalveluvelvoitteen tarjontaan alueellisesti haastavilla alueilla verrattuna siihen, että tarjonnan takaamiseksi pitäisi rakentaa uutta infrastruktuuria.

On tärkeää, että valtioneuvoston päätökset noudattavat eri selonteissa linjattuja toimintaperiaatteita.

Kyseessä on toimintavarma tekniikka ja Starlink on globaali vakavarainen ja liikevaihdoltaan merkittävä palveluntarjoaja, joka tarjoaa jo tällä hetkellä palveluitaan useassa kymmenessä maassa.

Toisin kuin Traficomien tuoreessa linjauksessa, satelliittilaajakaista tuleekin huomioida yleispalvelussa yhtenä turvaverkon toimijana erityisesti digikompassissa mainituissa tilanteissa alueellisen kattavuuden parantamiseksi, koska yleispalvelutilanteissa on yleensä kyse melko poikkeuksellista alueesta, jonne ei ole saatavilla kaupallista tarjontaa ilman lisätoimenpiteitä.

Energiamurros siirryttäessä päästöttömään energiatuotantoon

Yhteiskuntamme ei toimi ilman digitaalista infraa, jota taas ei ole olemassa ilman sähköä. Toisaalta myös sähköverkot ovat täysin riippuvaisia tietoliikenneyhteyksistä. Varautuminen mahdollisiin sähköpulan aiheuttamiin häiriöihin on Suomessa kansainvälisestikin poikkeuksellisen hyvä.

Kun sähkön hinta nousee, se lisää yhä enemmän painetta kehittää myös digitaalisen infran energiatehokkuutta. Uusi teknologia on entistä energiapihimpää. Hyvä esimerkki on mobiiliverkkojen sähkönkulutuksen kehittyminen. Verkossa siirretyn mobiilidatan määrä on reilussa viidessä vuodessa kuusinkertaistunut. Samaan aikaan datansiirron sähkönkulutus on laskenut 75 %. Kun energiasyöpöt 3G-verkot suljetaan vuoden 2023 jälkeen, odotettavissa on jälleen merkittävä parannus.

Tilastokeskuksen mukaan ICT-ala käyttää Suomessa 1,55 % kaikesta sähköstä, mutta sen osuus maamme kasvihuonepäästöistä on vain 0,04 %. Suomessa käytetty sähkö onkin pääosin hiiletöntä.

Ilmastonmuutoksen hillitsemiseksi on välttämätöntä, että yhteiskunnan vihreä siirtymä toteutuu. Digitalisaatio ja sähköistyminen ovat tärkeä osa tätä muutosta. Tiukat tavoitteet tarkoittavat koko energiasektorin myllerrystä seuraavan vuosikymmenen aikana. Digitaaliset energiantuotannon ohjausjärjestelmät kuluttavat sähköä vain murto-osan verrattuna siihen, kuinka paljon energiatehokkuus paranee.

Kriittisen infrastruktuurin haavoittuvuuden lisääntyminen

Selonteossa todetaan, että kriittisen infrastruktuurin suojaamiseksi tulisi kansallisella tasolla määritellä tarkemmin suojaamisen tavoitteet ja menettelytavat sekä julkisen ja yksityisen sektorin roolit ja vastuut. Myös kriittisen infrastruktuurin käsitettä ja kattavuutta tulisi säännöllisesti arvioida.

FiCom kannattaa avoimuuden uudelleentarkastelemista kriittisen infran osalta. Suomen huoltovarmuuden kannalta 1) ulkomaille suuntautuvat tietoliikenneyhteydet ovat elintärkeitä ja 2) kriittisen infran sijaintitietoja ei pidä kerätä yhteen valtiolliseen datapankkiin.

Merikaapelit siirtävät meren pohjassa valtavia määriä dataa. Niiden välityksellä kulkee käytännössä kaikki kansainvälinen viestintä. Kansallinen turvallisuus ja kyberturvallisuuteen liittyvät kysymykset ovat aina olleet merkityksellisiä, kun merikaapeliverkkoja on kehitetty ja rakennettu. Merikaapelin kriittinen vikaantuminen on varsin epätodennäköistä. Jos näin kuitenkin kävisi, internetin reititysprotokollat etsivät tietoliikenteelle automaattisesti uuden reitin. Kaikki tärkeimmät reitit on varmistettu, ja kaapeliyhteyksiä on useita.

Traficom antoi reilu vuosi sitten määräyksen, jossa kiristettiin merkittävästi merikaapeleiden suojaamista niiden rantautumiskohdissa. Määräyksen mukaan uudet merikaapelit on kaivettava vähintään kahden metrin syvyyteen vesirajan ja lähimmän rantautumiskaivon tai laiteaseman välillä. Jos rannan maaperä ei vaikkapa peruskallion vuoksi mahdollista maahan kaivamista, on suojaus tehtävä esimerkiksi koteloinnilla. Uudet kaapelit on myös haudattava metrin syvyyteen merenpohjaan vähintään viidensadan metrin matkalta niiden rantautumispaikasta. Jos tämä ei ole mahdollista, ne on suojattava esimerkiksi hiekkasäkeillä.

Viime keväänä kävi ilmi, että samaan aikaan, kun suojausvaatimuksia kiristetään, merikaapeleiden erittäin tarkka sijainti löytyy Traficom ylläpitämästä nettipalvelu [Oskarista](#). Toisin kuin kansainväliset kartat, esimerkiksi selonteossa käytetty [Submarine Cable Map](#), Oskari antaa erittäin tarkan sijaintitiedon merikaapeleiden rantautumispisteistä.

Taustana tietojärjestelmän rakentamiselle on ollut vuonna 2007 voimaan tullut INSPIRE-direktiivi, jolla pyritään estämään laivaliikenteen aiheuttamat vahingot kriittiselle infralle. Direktiivi on Suomessa implementoitu laiksi paikkatietoinfrastruktuurista. Sen mukaan aineisto voidaan säätää salassa pidettäväksi mm. yleisen turvallisuuden vuoksi. Lisäksi paikkatietoa hallinnoiva viranomais voisi asettaa ehtoja

paikkatietoaineiston katselulle, siirrolle tai käytölle. Näin ei kuitenkaan ole tehty, vaan tiedot ovat edelleen vapaasti saatavilla.

Tanskassa ja Virossa merikaapeleiden sijaintia koskevaa direktiiviä ei ilmeisesti ole samalla tavalla implementoitu, koska siellä ei vastaavaa avointa kaapeleiden sijainnin kertovaa tietopankkia ole.

Olisi järkevää, ettei Suomessakaan valtio tarjoaisi sijaintitietoja näin avoimesti ilman minkäänlaista kirjautumistakaan. Toivottavaa on, ettei uusien kaapeleiden sijaintitietoa enää jatkossa tarjota yhtä avoimesti.

Toinen esimerkki on Liikenne- ja viestintävirasto Traficom in toimeksiannosta parhaillaan valmisteltavana oleva **Sijaintitietopalvelu** on tietojärjestelmä, joka kerää kaikkien verkkoinfran omistajien datan sähköisessä muodossa yhteen lähteeseen. Jatkossa tiedot ovat siis edelleen hajautettuna verkon omistajilla näiden niin halutessaan mutta myös keskitetysti valtion tietojärjestelmässä.

Tietojärjestelmään kerätään kaapeleiden, putkien ja muiden aktiivisten verkon osien tarkat fyysiset sijainnit. Tietoliikenne-, sähkö-, kaukolämpö-, kaasu- ja viemäriverkot ovat tärkeä osa maamme kriittistä infrastruktuuria.

Sijaintitietopalvelun taustalla on yhteisrakentamisdirektiivin nojalla annettu yhteisrakentamislaki. Sen tarkoituksena on parantaa ja helpottaa olemassa olevien verkkojen sijaintitietojen saatavuutta ja siten vähentää infralle maarakennustöistä aiheutuvia vikatilanteita. Tietojen saaminen yhdeltä luukulta on kannatettava tavoite, mutta sen toteutustapa ei ole kestävä.

Erittäin tarkkojen infratietojen kokoaminen keskitettyyn järjestelmään yksityiskohtaisine sijaintitietoineen on valtava turvallisuusriski. Yhteiskunnan huoltovarmuuden kannalta keskeiset kriittiset infrakohteet ovat houkuttelevia iskukohteita kriisitilanteissa.

Viranomaiset vakuuttavat, että palvelu rakennetaan tietoturvallisesti. Järjestelmällä on kuitenkin tuhansia käyttäjiä, joilla on pääsy keskitettyihin tietoihin. Miten varmistetaan, että senttimetrin tarkkuudella saatavia kriittisen infran sijaintitietoja kyselevä taho on oikealla asialla?

Kun kaikkia tietoja hallinnoidaan samasta paikasta, koko palvelun käyttö voidaan lamauttaa, tai koko tietosisältö saattaa joutua väärin käsiin, jos se onnistutaan hakkeroimaan. Ukrainan esimerkki on osoittanut, että järjestelmien ja palveluiden hajauttaminen on tietoturvallisempi ratkaisu kuin niiden keskittäminen yhteen paikkaan.

Verkkotietojen kerääminen on hyvin kallis ja teknisesti erittäin vaativa tehtävä, mistä kertoo myös se, että Traficom in hanke on myöhästynyt selvästi alkuperäisestä aikataulustaan. Lisäksi verkkodatan jatkuva päivittäminen tulee vaatimaan resursseja ja luomaan kustannuksia sekä verkonomistajalle että Traficomille myös jatkossa. Sijaintitietopalvelun uudistaminen aiheuttaa lisäresurssitarpeita myös kunnille, jotka vastaavat asemakaava-alueiden yhdyskuntatekniikan sijoittamisen yhteensovittamisesta.

Suomessakin voitaisiin toteuttaa yhden luukun malli samalla tavoin kuin Ruotsissa. Siellä sikkalainen viestintävirasto vastaanottaa keskitetysti tietopyynnot urakoitsijoilta ja lähettää ne tarvittaessa eteenpäin sijaintitietopalvelun tarjoajalle kartta- tai kaapelinäyttöjä varten. Verkkotiedot sijaitsevat ainoastaan verkonomistajien järjestelmissä.

Elina Ussa
toimitusjohtaja
FiCom ry