ERILLISVERKOT

Turvallisuuskriittisen teknologian trendit 2022 -katsaus

4.5.2022

Johdanto

Erillisverkkojen toisessa teknologiatrendit -katsauksessa aiheena on erityisesti Ukrainan sota tietoliikenteen ja mobiiliverkkojen näkökulmasta. Tarkastelemme myös erilaisia kehittyviä avaruuspalveluja ja niiden mahdollisuuksia viranomaisille ja turvallisuustoimijoille.

Venäjän aloittama hyökkäyssota Ukrainassa on vaikuttanut Euroopan turvallisuustilanteeseen. Vakava ja vaikea tilanne heijastuu väistämättä myös keskusteluun ja näkemyksiin suomalaisten viranomaisten ja turvallisuustoimijoiden kriittisistä ict-työvälineistä ja yhteyksistä. Tässä Erillisverkkojen Turvallisuuskriittisen teknologian trendit 2022 -katsauksessa keskeisiä tarkastelun aiheita ovat:

- Ukrainan sota ja sen heijastuminen tietoliikennekysymyksiin erityisesti mobiiliverkkojen toimintavarmuudesta ja turvallisuudesta
- avaruusteknologia ja -palvelut turvallisuustoimijoiden näkökulmasta.

Ukrainan mobiiliverkot toimivat edelleen odotettua paremmin

Niin kansalaiset kuin viranomaisetkin tarvitsevat kriiseissä ja poikkeusoloissa kyvykkyyden kommunikointiin. Tietoverkoilla ja mobiilipalveluilla on operatiivinen rooli sotatilanteessa, mutta ne myös auttavat kansalaisia kriisinsietämisessä. Ihmiset pystyvät viestimään välimatkoista huolimatta, voivat olla yhteydessä ystäviin ja sukulaisiinsa sekä saavat tietoa tilanteen etenemisestä. Mobiiliverkkojen avulla viranomaiset voivat helposti ja nopeasti saavuttaa kansalaiset sekä varoittaa ja ohjeistaa. Tärkeää on myös luoda uskoa ja nujertaa propagandaa.

Ukrainassa jopa väestönsuojiin levitetyt puhelin- ja internet-yhteydet ovat lisänneet kansalaisten henkistä kriisinkestävyyttä. Myös olemassa olevat lankapuhelinyhteydet toimivat varmentavana viestiyhteytenä.

Ukrainassa mobiilipalveluiden toiminta vaikuttaa olevan kohtuullisella tasolla maan itäisimpiä osia lukuun ottamatta. Esimerkiksi presidentti **Volodymyr Zelenskyi** on pystynyt tehokkaasti hyödyntämään tietoliikenneyhteyksiä ja muun muassa sosiaalista mediaa vaikuttamisen välineenä. Ukraina on pystynyt välittämään kansainväliselle yleisölle tilannekuvaa tapahtumista ja sodan etenemisestä.

Ukrainassa on tehty pitkäjänteistä varautumista

Ukrainan yhteiskunnan varautumista on kehitetty vuodesta 2014 lähtien Venäjän generoiman Itä-Ukrainan sodan myötä. Tämä koskee niin tietoliikennettä kuin mobiiliviestintääkin.
Tällä hetkellä myös hyökkääjä käyttää hyödykseen kaupallisia mobiilipalveluita. Venäjä ei ole systemaattisesti tuhonnut Ukrainan mobiiliverkkoja, koska se käyttää niitä itsekin.
Vaikka Ukrainan mobiiliverkot ovat kärsineet siirtoyhteyksien katkeamisista, tukiasemien tuhoutumisesta sekä sähkökatkoista, verkot ovat selvinneet tähän asti ennakoitua paremmin.
Taustalla on Ukrainan hyvä varautuminen ja Itä-Ukrainan sodan kokemusten hyödyntäminen.
Sodan alkaessa maassa toteutettiin kansallinen roaming eli verkkovierailu, ja verkkojen korjaustoimintaa tehdään ilmeisen kunnianhimoisesti sodan oloissakin.
Erillisverkot seuraa Ukrainan sotaa erityisesti oman toimialamme näkökulmasta. Erillisverkkojen tietojen mukaan viranomaisilla Ukrainassa on käytössä erillisiä anologisia ja digitaalisia viestintäjärjestelmiä, mutta Suomen viranomaisverkko Virven tapaista

viranomaisverkkoa maassa ei ole. Lähtötilanne on siis Suomeen verrattuna erilainen, sillä meillä maanlaajuista Virveä käyttävät kaikki viranomaiset ja turvallisuustoimijat. Virveä kehitetään aktiivisesti, ja se siirtyy tulevaisuudessa Tetra-pohjaisesta verkosta laajakaistaiseksi.

Toimivat mobiiliverkot yhdistävät viranomaiset ja kansalaiset

Mobiiliverkkojen toimintakyky on eduksi Ukrainan puolustustaistelulle, koska kansalaiset voivat antaa tietoa vihollisen liikkeistä ja taisteluiden aiheuttamista vaurioista. Käytännössä tämä tarkoittaa esimerkiksi aktiivista tilannetietojen tai videoiden toimittamista viranomaisille tai vihollisen hallussa olevan alueen web-kameroiden hyödyntämistä. Ukraina hyödyntää myös ainakin jossain määrin joukkoistettua tiedustelutiedon keräämistä. Tämä edellyttää luonnollisestikin toimivia matkapuhelinverkkoja. Venäläiset katkaisivat vappuna Etelä-Ukrainassa miehittämiltään alueilta internet ja matkapuhelinyhteydet. Ne palautettiin osittain toimimaan noin vuorokauden viiveellä Venäjän tietoverkkojen kautta. Näin käyttäjät joutuvat Venäjän internet-kuplaan.

Merkittävä oivallus Ukrainassa on ollut pääkaupunki Kiovan matkalippu- ja pysäköintisovelluksen valjastaminen väestönsuojelun tietokanavaksi. Laajalti käytössä olevan sovelluksen avulla varoitetaan ja informoidaan kansalaisia. Sovelluksella voi myös raportoida sotarikoksista. Sovelluksen käyttötarkoituksen muutos toteutettiin yvin nopeasti heti sodan alettua.

Jo ennen sodan alkamista ja sodan alkuvaiheissa Ukrainassa toteutettiin erilaisia toimenpiteitä mobiiliverkkojen varmistamiseksi. Verkkojen kapasiteettia kasvatettiin, venäläisten ja valkovenäläisten SIM-korttien käyttö ja yhteydet Venäjälle estettiin. Myös kansallinen roaming otettiin käyttöön.

”Ketju on yhtä vahva kuin sen heikoin lenkki”

Venäjä käyttää Ukrainan matkapuhelinverkkoa ja tavallisia radiopuhelimia paikkaamaan omia ilmeisen vakavia viestintäjärjestelmiin ja niiden käyttötaitoon ja motivaatioon liittyviä heikkouksiaan. Venäläisillä on käytössään ukrainalaisia SIM-kortteja, mutta Venäjälle suuntautuvien yhteyksin katkaisemisen vuoksi venäläiset voivat käyttää niitä vain Ukrainan

alueella tapahtuvaan viestintään (pois lukien tilanne, jossa käytössä on jonkinlainen releointilaitteisto). Venäjä hyödyntää näitä viestintätapoja ainakin osittain eikä pyri salaamaan viestintäänsä (esimerkiksi VHF-puhelimien käyttö johtamisessa). Ukraina ja sen läntiset kumppanit pystyvät jossakin määrin seuraamaan reaaliaikaisesti venäläisten viestintää ja hyödyntämään tätä operatiivisesti.

Venäläiset ovat pakotettuja käyttämään viestintäjärjestelmää, jonka käyttö onnistuu kaikilta kuhunkin operaatioon osallistuvalta joukoilta. Venäläisten käytössä olevien salattujen yhteyksien etua menetetään, jos osa tiedon kulusta tapahtuu salaamatonta väylää myöten koska ”ketju on yhtä vahva kuin sen heikoin lenkki”.

Ukraina haluaa hyödyntää avaruusteknologiaa ja satelliittipalveluita

Sekä julkiset että yksityisen sektorin toimijat ovat yhä kiinnostuneempia satelliittipalveluista. Muun muassa kehittyvä teknologia ja alentuneet logistiset kustannukset ovat lisänneet erilaisten satelliittipalveluiden (esim. matalan kiertoradan satelliittipalvelut, LEO) saatavuutta. Kiristynyt turvallisuustilanne vaikuttaa myös kiinnostukseen, koska turvallisuustoimijoille uudet palvelut lupaavat esimerkiksi entistä tarkempaa tilannekuvaa.
Ukrainan sodan yhtä merkittävää avaruuspalveluhankintaa pystyi seuraamaan Twitterissä, kun Ukrainan varapääministeri **Mykhailo Fedorov** pyysi toimitusjohtaja, vaikuttaja **Elon Muskilta** apua Twitterissä (26.2.2022). Musk suostui pyyntöön ja aktivoi käytännössä välittömästi Starlink-palvelunsa Ukrainassa. Lisäksi Ukrainaan lähettiin arvioiden mukaan noin 5000 palvelun käyttöön tarkoitettua päätelaitetta. Starlink on Elon Muskin perustaman Space X -yrityksen tietoliikennesatelliittipalvelua tarjoava yhtiö. Julkisuudessa olleiden tietojen mukaan tällä hetkellä Ukrainassa on käytössä yhteensä noin 10 000 Starlink-päätelaitetta.

Melko pian lanseeraamisen jälkeen Starlink-palvelua estettiin jamming-menetelmällä, jossa palvelun käyttämää taajuutta lähetetään häirintälaitteilla. Näin estetään palvelun toimivuus. Lisäksi arveltiin, että vastaanottimia käytetään maalittamiseen, eli Venäjä pyrki havaitsemaan vastaanottimen käyttäjän sijainnin. Musk kertoi häirintäongelman poistuneen uusimman ohjelmistopäivityksen myötä. Päivitys liittynee satelliitin ja asiakaslaitteen väliseen taajuuskäyttöön. Tämän onnistumisesta liikkuu kahtalaista tietoa, mutta totuus lienee jossain ääripäiden välillä. Estoa on saatu vähennettyä, mutta ei täysin poistettua.

Ukrainan vapautettua alueita takaisin omaan hallintaansa, alkoi myös tietoliikennepalveluiden palauttaminen. Tuhotun infrastruktuurin myötä tuhoutuneet olivat myös osa tukiasemien kiinteistä tietoliikenneyhteyksistä, jotka vaaditaan, jotta tukiasemaa toimii. Näitä tuhoutuneita yhteyksiä on Ukrainassa korvattu Starlinkin avulla.

Viime aikoina on uutisoitu myös siitä, kuinka Ukraina käyttää puolustustaisteluissa Starlink-palvelua hyväkseen droonioperaatioissa. Droonit eivät itsessään pysty kommunikoimaan satelliittipalvelun kanssa, mutta Starlink mahdollistaa tehokkaamman yhteistyön drooneja ohjaavien joukkojen ja esimerkiksi tykistön välillä.

Satelliittipalveluiden merkitys turvallisuudelle tunnistettu laajasti Euroopassa

Euroopan unioni julkisti helmikuussa hankkeen, joka tähtää eurooppalaisen tietoliikennesatelliittipalvelun kehittämiseen. Tavoitteena on aloittaa palvelun kehittäminen 2023, ja käyttövalmis palvelun pitäisi olla vuonna 2028. Aikataulu kuulostaa vähintäänkin kunnianhimoiselta. Komissio on arvioinut hankkeen kustannuksiksi kuusi miljardia euroa. Palvelun käyttökohteeksi mainitaan muun muassa kriittinen infrastruktuuri, kuten sähköverkot, rajaturvallisuus ja kriisinhallinta sekä palvelu niillä alueilla, joissa maanpäälliset mobiiliverkot eivät syystä tai toisesta toimi.

Energiasektori on mielenkiintoinen ja tärkeä toimiala avaruuspalveluiden näkökulmasta. Samaan aikaan, kun Ukrainan sota käynnistyi ja keskustelu EU:n energiaomavaraisuudesta käynnistyi, tehtiin kyberisku globaaliin satelliittipalveluntarjoajaan. Isku katkaisi muun muassa etäyhteydet joihinkin tuulivoimaloihin Saksassa. Voi olla, että energiasektori oli iskun sivullinen uhri – keskeisempi pyrkimys iskulla oli häiritä Ukrainan asevoimien toimintaa.

Suomi on hereillä uusien avaruuspalveluiden osalta

Valtioneuvosto julkaisi maaliskuussa 2022 selvityksen avaruustoiminnan yhteiskunnallisista vaikutuksista. Selvityksessä satelliittiteknologialla todetaan olevan yhä suurempi strateginen merkitys yhteiskunnan toimivuudelle, kansalliselle turvallisuudelle ja eri hallinnonalojen päätöksenteolle. Satelliittiteknologialla nähdään olevan merkitystä myös suomalaiselle teollisuudelle. Suomeen on syntynyt paljon langattoman tiedonsiirron osaamista, joka soveltuu

myös satelliittiratkaisujen kehittämiseen ja kaupallistamiseen.

Teknologisesti mielenkiintoisia ovat myös Non-Terrestial-Networks -ratkaisut, joissa matkapuhelimet ja muut mobiililaitteet kytkeytyvät suoraan satelliittipalveluun, kun maanpäällinen verkko ei ole käytössä. Näiden standardisointi etenee osana 3GPP:n yhteistyöjärjestön 5G- ja 6G-määrittelyä. Näiden ratkaisujen saatavuus Suomen alueella on vielä vuosien päässä, mutta parhaimmillaan ne voisivat täydentää maanpäällisiä verkkoja. Kun nämä teknologiat ovat käytössä, infrastruktuurin tuhoaminen ja samalla väestön tiedonsaamisen estäminen on nykyistä hankalampaa.

Uudet tietoliikennesatelliitit eivät korvaa Virve 2 -palvelun käyttämää radioverkkopalvelua, mutta voivat täydentää ja varmentaa sitä. Parhaimmassakin palvelussa on heikkoutensa, ovathan esimerkiksi aluevesirajojen ulkoreunat haastavia mobiiliverkoille.

Kun puhumme satelliiteista, on tässä ajassa tärkeä nostaa esiin myös aika- ja paikannusratkaisut. Ukrainan sota oli jo käynnissä, kun Kaakkois-Suomessa koettiin laajamittaisia häiriöitä gps-paikannuspalveluissa. Häiriöt vaikuttivat jonkin verran muun muassa lentoliikenteeseen. Sijaintitiedon epäluotettavuus vaikuttaa myös turvallisuustoimijoiden arkeen. Toimintaa johdetaan tilannekuvan perusteella, jonka tärkeimpiä tietovirtoja on eri yksiköiden sijainti. Häiriöiden minimoimiseksi Suomessa ollaan vuosikymmenen puolivälin paikkeilla ottamassa käyttöön Galileo-paikannuspalvelun toimintavarmempi PRS-palvelu. Palvelun vastuuviranomainen on Liikenne- ja viestintävirasto Traficom, ja palvelun tuottajana toimii Erillisverkot.

Viranomaistehtävään osallistuvien yksiköiden sijaintitieto on yksi tärkeimmistä tilannekuvan tietovirroista, Galileo PRS parantaa sijaintitiedon saatavuutta ja luotettavuutta.

Katse on taivaalla, jalat maassa

Tällä vuosikymmenellä satelliittiratkaisujen merkitys yhteiskunnalle lisääntyy olosuhteista riippumatta. Turvallisuustoimijoille palveluiden saatavuus aikaan ja paikkaan katsomatta, kaikissa olosuhteissa on tärkeää, ja siksi myös satelliittiratkaisujen kehitystä seurataan silmä kovana. Tällä hetkellä liikkeellä on monia eri toimijoita ja teknisiä ratkaisuja. Herääkin kysymys, voivatko ne kaikki menestyä kaupallisesti. EU-komission työltä odotetaan paljon, ja uskomme, että siinä turvallisuustoimijoiden erityistarpeet tulevat huomioiduksi kaikkein parhaiten.

Vaikka katse on taivaalla, jalat on pidettävä maassa.

Turvallisuuskriittisen teknologian trendit 2022 -katsaus perustuu Erillisverkkojen omaan arvioon, asiakashaastatteluihin sekä aktiiviseen teknologiakehityksen seuraamiseen ja vuoropuheluun viranomaisten ja muiden turvallisuustoimijoiden kanssa. Turvallisuuskriittisen teknologian trendit -katsaus ilmestyy kerran puolessa vuodessa ja avaa teknologianäkymiä tarkemmalla tasolla erikseen valitusta näkökulmasta. Vuoden 2021 katsauksessa teemana olivat teknologioiden konvergoituminen, 5G, pilviteknologiat ja tekoäly ja satelliitit.

Lisätietoja

Antti Kauppinen, teknologiajohtaja, antti.kauppinen@erillisverkot.fi
Tomi Lounema, johtava asiantuntija, tomi.lounema@erillisverkot.fi
Katariina Salmisalo, viestintäjohtaja, katariina.salmisalo@erillisverkot.fi

Suomen Erillisverkot Oy
PL 357, Tekniikantie 4 B
02151 Espoo
Puhelin 0294 440 500
erillisverkot.fi