Martti Lehto, Jyväskylän yliopisto
6.10.2021

Valtioneuvoston puolustusselonteko

Asia: VNS 8/2021 vp

1. Digitalisaatio muuttaa turvallisuusympäristöä

Yhteiskunnan yksityiset ja julkiset palvelut perustuvat yhä laajemmin ihmisten, erilaisten toimijoiden ja älykkäiden systeemien keskinäisriippuvaan toimintaympäristöön. Digitaalitalouden kehitystä edistävät erilaisten palveluiden ja tietokäytäntöjen digitalisoituminen ja siirtyminen verkkoon. Yhteiskunnan digitalisaatio on vahvistanut kybertoimintaympäristöä, luonut kybertilan, jossa kriittinen infrastruktuuri tuottaa yhteiskunnan elintärkeät palvelut pääosin digitaalisesti. Tämä digitaalinen murros muuttaa tapaa, jolla palveluita ja hyvinvointia tuotetaan eli koko yhteiskunnan toimintalogiikka on muuttunut – kyber on kaikkialla.

EU:n turvallisuusunionistrategiassa (2020) todetaan, että ”kyberhyökkäyksillä on huomattavia haittavaikutuksia koteihin, pankkeihin, rahoituspalveluihin ja yrityksiin. Fyysisten ja digitaalisten järjestelmien keskinäinen riippuvuus pahentaa mahdollisia vahinkoja entisestään: kaikilla fyysisillä iskuilla on vaikutusta digitaalisiin järjestelmiin, ja tietojärjestelmiin ja digitaalisiin infrastruktuureihin kohdistuvat kyberhyökkäykset voivat lamauttaa keskeisiä palveluita.”

2020-luvun kybermaailman suurimmat taistelut käydään ihmisten mielissä. Informaatio-operaatioiden avulla tavoitellaan sodan voittamista käyttäen mahdollisimman vähän aseellista voimaa. Informaatio-operaatiossa on tarkoitus vaikuttaa siihen, miten ihmiset ajattelevat ja toimivat. Strategisesta kommunikaatiosta onkin tullut valtioille toimintatapa, jolla ne pyrkivät luomaan kansallista turvallisuutta ja kansakunnan yhtenäisyyttä sekä vahvistamaan tarvittavia uhkakuvia kansalaisten ja sotilaiden mielissä. Strategisen kommunikaation paradigmassa koko maailma on kybertaistelutila, jossa informaatiota on vaikea hallita. Sosiaalisen median eri muodot ulottuvat taistelukentälle ja se haastaa valtiollisen kontrollin.

2. Kyber-, informaatio- ja avaruuspuolustus

Valtioneuvoston vuoden 2017 puolustusselonteossa todetaan ” Suomen puolustaminen edellyttää kykyä toimia maa-, meri-, ilma- ja kybertoimintaympäristössä.” Tuolloin kyberpuolustus oli kuvattu osana puolustusjärjestelmän yhteisiä suorituskykyjä. Em. selonteossa informaatio- ja avaruuspuolustus olivat mukana yleisinä mainintoina.

Uusin selonteko nostaa Kyber-, informaatio- ja avaruuspuolustuksen uudelle tasolla tehden niistä perinteisten maa-, meri- ja ilmapuolustuksen rinnalle tasavertaisen toimintaympäristön. Tämä vastaa monessa maassa olevaa jakoa sillä erolla, että informaatiopuolustus on erotettu omaksi toimintaympäristöksi kybertoimintaympäristöstä. Tätä Suomen tekemää jakoa voidaan pitää hyvänä ja selkeyttävänä ratkaisuna.

2.1 Kyberpuolustus

Globalisaatio ja internet ovat antaneet yksilöille, organisaatioille ja valtioille uusia mahdollisuuksia toimia digitalisoituvassa kybermaailmassa. Tämän päivän sekä tulevaisuuden poliittisissa ja sotilaallisissa konflikteissa on mukana kyberelementti, jonka tarkkaa vaikuttavuutta poliittisten tavoitteiden saavuttamisessa on vaikea ennustaa.

Kybertaistelukentällä toimijan koolla ei ole samanlaista merkitystä kuin fyysisessä maailmassa – sekä suuret että pienet voivat olla tehokkaita. Miten ”kybervoima” (cyber power eli kyberkyvykkyydet valtaelementtinä) tulee maailmassa jakaantumaan eri valtiollisten kuin ei-valtiollisten toimijoiden kesken on erilaisia arvioita. Suurvalloille on mahdollista investoida laaja-alaisiin puolustuksellisiin ja hyökkäyksellisiin kyvykkyyksiin, kun taas pienet valtiot keskittyvät erikoisosaamiskykyihin.

Kybertilannetietoisuuden kehittäminen

EU komissio toteaa uusimmassa kyberturvallisuusstrategiassaan (2020), ettei ”EU:lla ole kollektiivista tietoisuutta kyberuhista. Tämä johtuu siitä, että kansalliset viranomaiset eivät kerää ja jaa järjestelmällisesti tietoja, kuten yksityiseltä sektorilta saatavaa tietoa, mikä voisi auttaa arvioimaan kyberturvallisuuden tilaa EU:ssa. Jäsenvaltiot ilmoittavat vain murto-osasta tapauksista, eikä tietojen jakaminen ole järjestelmällistä eikä kattavaa.”

Selonteon mukaan ”Puolustusvoimat on kehittänyt kybertilannekuvan muodostamista.” Selonteossa on esitetty, että ”Puolustusjärjestelmän kybertilannekuvan parantaminen sekä kyberuhkien estäminen ja torjuminen edellyttävät tiedonvaihdon, toimivaltuuksien ja kansallisten yhteistyörakenteiden kehittämistä viranomaisten välillä. Viranomaisyhteistyön kehittämistarpeet on selvitettävä ja määriteltävä muutosten perusteiksi.” Esitystä on pidettävä perusteltuna ja se tukee EU:n kyberturvallisuusstrategiassa esitettyjä vaatimuksia.

Kansallinen kybertila/kybertoimintaympäristö tulee määritellä

Selonteko edellyttää, että ” Aluevalvontalakia (755/2000) ja siihen liittyviä säädöksiä on tarkistettava vastaamaan Suomen kansainvälisen yhteistyön ja harjoitustoiminnan tarpeita.” Tarve uudistukselle voidaan nähdä kybertoimintaympäristön näkökulmasta,

josta puuttuu selkeä ja tarkkarajainen juridinen määrittely kansallisesta kybertoimintaympäristöstä.

Kybertoimintaympäristö poikkeaa perinteisestä kansallisesta toimintaympäristöstä, jossa itsenäisellä valtiolla on määritellyt maantieteelliset rajat, jotka määrittävät valtion kansallisen alueen (maa-alueen, vesialueen ja ilmatilan) eli valtion toimivallan alueen.

Aluevalvontalaki (18.8.2000/755) kuvaa Suomen valtakunnan aluetta määrittelemällä maa- ja merirajoja ja niiden yläpuolista ilmatilaa. Siten Suomen alueellisen koskemattomuuden valvonta kohdistuu Suomen rajoille. Suomen alueellisen koskemattomuuden turvaamisessa käytetään voimakeinoja tai muita toimenpiteitä alueloukkauksen estämiseksi tai torjumiseksi.

Kansallinen kybertila tulisi määritellä, jotta voitaisiin toteuttaa Suomen kybertilan koskemattomuuden valvonta ja torjunta. Tarvitaan selkeä määrittely kansallisesta suvereniteetista kybertilassa. Tämä tila ei ole vain teknologinen toimintaympäristö vaan merkittävällä tavalla turvallisuuspoliittinen toimintaympäristö.

2.2 Informaatiopuolustus

Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko (2020) mainitsee informaatiovaikuttamisen osan globaaleja haasteita ja toteaa, että kyberpuolustuksen kehittämisen lisäksi toimintaympäristön muuttuminen korostaa tarvetta informaatiopuolustuksen eli väärän tiedon oikaisemisen ja tiedon eheyden varmistamisen laaja-alaiselle kehittämiselle.

Informaatiosodankäynti on yhteiskunnalliseen ja sotilaalliseen päätöksentekoon ja toimintakykyyn sekä kansalaisten mielipiteisiin vaikuttamista eli informaatioylivoiman hankkimista. Jo rauhan aikana informaatiovaikuttamisella pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn eri kampanjoiden avulla. Informaatiotilaa hallitaan jo rauhan aikana, jotta tarvittaessa se voidaan ottaa kokonaan haltuun osana sodan ajan muita operaatioita strategisten tavoitteiden saavuttamiseksi. Erityisesti sosiaalisen median alustat antavat mahdollisuuden informaatiovaikuttamiselle ja informaatiotilan hallinnalle.

Informaatiotilan hallinta näkyy erityisesti yksinvaltaisesti johdetuissa maissa kuten Venäjä, Kiina, Pohjois-Korea, Valko-Venäjä, Iran, joissa valtiojohto pyrkii eri keinoin hallitsemaan ja valvomaan internettiä ja sen palveluita.

Eri toimijat yhteiskunnassa pyrkivät omilla vastuualueillaan torjumaan disinformaatiota, sekä aggressiivista ja anonyymiä vaikuttamista Internetissä. Tässä

riippumaton, itsenäinen media on avainasemassa ja osa yhteiskunnan informaatiopuolustusta.

Euroopan komission tiedonannossa (Yhteinen kehys hybridiuhkien torjumiseksi, 2016) todetaan, että ”On hyvin tärkeää, että hybridiuhkiin kyetään vastaamaan pätevällä strategisen viestinnän strategialla. Yhteiskunnan valmiuksia vastata hybridiuhkiin voidaan parantaa ensisijaisesti antamalla nopeasti asiatietoihin perustuvia vastauksia ja lisäämällä yleistä tietoisuutta.”

Puolustusselonteossa todetaan, että ”Informaatiopuolustuksen päämäärä on suojata maanpuolustuksen toimintoja ulkoa ohjatun ja muun vahingoittamistarkoituksessa tehdyn viestinnän vaikutuksilta.” Kehittämisen osalta keskeistä on kyetä yhteensovittamaan eri toimintatavat viranomaisten ja muiden toimijoiden kesken vaikuttavan reagoinnin vaatimalla nopeudella. Suorituskykyjen kehittämisessä korostuu yhteistoiminta kaikkien viranomaisten ja kansainvälisten kumppanien kanssa. Kehittämisessä tulee ottaa huomioon koko valtiohallinnon informaatiovaikuttamiseen vastaamiseen liittyvät toimet ja ajan tasalla olevat toimivaltuudet.

Tarvitaan kansallinen informaatiovaikuttamisen torjunnan/informaatiopuolustuksen ohjelma, jonka avulla varmistettaisiin yhteiskunnan toimintakyky sekä normaaliaikoina että poikkeusoloissa. Ohjelman tulisi tuottaa informaatiovaikuttamisen torjunnan/informaatiopuolustuksen kansallisen strategisen johtamisen rakenteet ja vastuun jakamisen periaatteet.

2.3 Avaruuspuolustus

Suomessa ensi kertaa avaruuspuolustus otetaan mukaan selkeäksi osaksi puolustuspolitiikkaa. Yhdysvallat perusti joulukuussa 2019 itsenäiset avaruuspuolustusjoukot. Niiden tehtävä on turvata suurvallan avaruudessa olevaa omaisuutta, kuten satoja satelliitteja, joita käytetään tiedusteluun ja viestintään. Suurvallat kehittävät myös offensiivisia avaruussuorituskykyjä.

Nykyään Maata kiertää arviolta alle 3 000 toiminnassa olevaa satelliittia. Yksi esimerkki alan erittäin nopeasta kasvusta on Elon Muskin avaruusyhtiö SpaceX:n Starlink-satelliittien megakonstellaatio sisältää jo noin 1700 tietoliikennesatelliittia. Yhtiö on hakenut lupaa jopa 40 000 satelliitin lähettämiseen. Starlink-järjestelmän tehtävänä on tarjota nopea internetyhteys kaikkialle maapallolla. Toiminta osoittaa avaruustoiminnan kasvunopeutta.

Monet kansalliset palvelut ovat riippuvaisia avaruuspohjaisista aika- ja paikkatiedoista. Eurooppalaisen Galileo-satelliittijärjestelmän PRS-palvelun (Public Regulated Service) on

tarkoitus tuottaa EU:n jäsenvaltion viranomaisille paikannus- ja aikatietoa, joka antaa salatun ja vahvan lähetyssignaalin ansiosta suojaa kyberhyökkäyksiä vastaan.

Puolustusvoimat on yhä riippuvaisempi avaruudellisista toimintakyvyistä. Siksi ajantasaisella avaruustilannekuvalla lisätään yhteiskunnan ja puolustusjärjestelmän suojaa sekä edistetään avaruuden turvallisuutta ja kestävää käyttöä.

Avaruustilannekuvan kehittäminen edellyttää vahvaa yhteistoimintaa muiden maiden kanssa. Tästä on osoituksena Suomen ja Yhdysvaltain 4.11.2019 allekirjoittama avaruustilannekuvayhteistyötä koskeva yhteisymmärryspöytäkirja. Avaruudessa on niin kaupallista, tieteellistä kuin sotilaallista toimintaa ja sitä pitää pystyä valvomaan organisoidusti.

Suomen tulee luoda riittävät osaamis- ja investointiresurssit avaruuspuolustuksen toteuttamiselle yhteistoiminnassa kansallisten ja kansainvälisten toimijoiden kanssa.

3. Uudet teknologiat auttavat suorituskykyjen kehittämisessä

Puolustusselonteossa todetaan uusien teknologioiden kuten tekoälyn, koneoppimisen ja sensoriteknologioiden vaikuttavan puolustuksen kaikkiin toimintaympäristöihin, mutta sen vaikutukset kohdistuvat etenkin kyber-, avaruus- ja informaatiopuolustukseen. Uusia teknologioita tullaan hyödyntämään sotilaallisesti esimerkiksi informaation käsittelyssä, eri tilannekuvien muodostamisessa, asejärjestelmien ohjauksessa ja logistiikassa. Lisäksi tekoälyn avulla voidaan tukea päätöksentekoa tarkemmalla ja nopeammin käyttöön saatavalla tiedolla.

Suomella on mahdollisuus kehittyä merkittäväksi toimijaksi uusien teknologioiden soveltamisen alueella. Tämä edellyttää riittäviä panostuksia sekä osaamiseen että taloudellisiin resursseihin.

4. Lopuksi

Hallitusohjelmassa on asetettu tavoitteeksi, että Suomi tunnetaan edelläkävijänä, jossa digitalisaation ja teknisen kehityksen tuomia mahdollisuuksia kehitetään ja otetaan käyttöön yli hallinto- ja toimialarajojen. Tavoitteena on nostaa julkisen sektorin teknologia- ja digitalisaatiokyvykkyyttä sekä kehittää julkisen ja yksityisen sektorin yhteistyötä.

Digitalisaatiokehitys lisää valtiollisten ja valtiosta riippumattomien toimijoiden mahdollisuuksia tehdä yhä kehittyneempiä kyber- ja informaatio-operaatioita. Niissä yhteiskunnan haavoittuvuuksia hyödynnetään kriittisen infrastruktuurin sabotoimiseksi ja tuhoamiseksi. Informaatiovaikuttamisella tavoitellaan sotilaallisia ja poliittisia tavoitteita. Siksi puolustuselonteon kyber-, informaatio- ja avaruuspuolustuksen kehittämisen tavoitteita on pidettävä välttämättöminä, jotta pystytään turvaamaan

yhteiskunnan elintärkeitä toimintoja normaaliaikoina, normaaliaikojen häiriötilanteissa ja poikkeusoloissa. Kehittäminen edellyttää taloudellisia investointeja järjestelmäkehitykseen ja osaamispääoman kasvattamiseen.

Työelämäprofessori, ST Martti Lehto

Jyväskylän yliopisto, Informaatioteknologian tiedekunta

martti.lehto@jyu.fi