Martti Lehto, Jyväskylän yliopisto
26.10.2021

Eduskunnan puolustusvaliokunta

Asia: Valtioneuvoston puolustusselonteko, VNS 8/2021 vp

Valtioneuvoston selonteko sisäisestä turvallisuudesta, VNS 4/2021 vp

1. Digitalisaatio muuttaa turvallisuusympäristöä

Yhteiskunnan yksityiset ja julkiset palvelut perustuvat yhä laajemmin ihmisten, eri toimijoiden ja älykkäiden systeemien keskinäisriippuvaan digitaaliseen toimintaympäristöön. Digitaalitalouden kehitystä edistävät erilaisten palveluiden ja tietokäytäntöjen digitalisoituminen ja siirtyminen verkkoon. Yhteiskunnan digitalisaatio on luonut kybertilan, jossa kriittinen infrastruktuuri tuottaa yhteiskunnan elintärkeät palvelut yhä laajemmin 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 digitaalisen maailman suurimmat taistelut käydään ihmisten mielissä. Informaatio-operaatioiden avulla tavoitellaan informaatioympäristön hallintaan ja operaatioissa 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 taistelutila, jossa informaatiota pyritään hallitsemaan sen haasteellisuudesta huomimatta.

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 puolustusselonteko nostaa kyber-, informaatio- ja avaruuspuolustuksen uudelle tasolle tehden niistä perinteisten maa-, meri- ja ilmapuolustuksen rinnalle tasavertaisen toimintaympäristön. Vastaavasti sisäisen turvallisuuden selonteossa on

erikseen analysoitu kyber- ja informaatioympäristöä. Tämä vastaa monessa muussa maassa olevaa jakoa sillä erolla, että informaatiopuolustus on erotettu omaksi toimintaympäristöksi kybertoimintaympäristöstä. Tätä Suomen tekemää jakoa voidaan pitää hyvänä ja selkeyttävänä ratkaisuna digitaalisen maailman ilmiöiden ymmärtämisessä.

2. Hybridipuolustus

Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko (2020) otti esille hybridivaikuttamisen. Sen mukaan ”Hybridivaikuttaminen on lisääntynyt ja monimuotoistunut, minkä takia siitä on tullut aiempaa suurempi turvallisuusuhka.”

Hybridivaikuttamisen keinovalikoimaan kuuluvat mm., diplomaattiset, taloudelliset ja sotilaalliset keinot sekä informaatio- ja kybervaikuttaminen. Hybridioperaatioita toteuttavat ensisijaisesti valtiolliset toimijat. Vastustajille on äärimmäisen houkuttelevaa kokeilla hybridioperaatioiden eri menetelmiä jo nyt, koska niissä on suhteellisen pieni kiinnijäämisriski verrattuna perinteisiin sotilaallisiin operaatioihin tai muihin vaikuttamismenetelmiin.

Hybridioperaatioiden havaitseminen ja estäminen olisi tehtävä varhaisessa vaiheessa, ennen kuin hyökkääjä ottaa käyttöönsä koko hybridimenetelmien arsenaalin. Hybridioperaatioiden havaitsemiskykyä (varhaisvaroitus) on parannettava, jotta vastustajan toiminta ja vaikuttamisyritykset voidaan lopettaa ennen kuin ne ovat kunnolla alkaneetkaan.

Puolustusselonteossa hybridiuhkakokonaisuutta lähestytään sotilaallisesta näkökulmasta, jolla Puolustusvoimat tarkoittaa laaja-alaista vaikuttamista. Siinä hybridivaikuttamisen uhkakuvaan sisältyy myös avoin sotilaallinen voimankäyttö osapuolten välillä. Puolustusvoimille hybridipuolustus käsittää laajaa sotilaallisen voimankäytön spektriä eri uhkaympäristöissä.

Hybridisodankäynnistä on esimerkkejä, jossa kineettistä sodankäyntiä on jatkettu matalan intensiteetin kineettisten ja ei-kineettisten operaatioiden avulla. Venäjän sotatoimet Ukrainassa vuonna 2014 ovat esimerkki sodankäynnistä, jossa erikoisjoukkojen rajoitetun voimankäytön, poliittisen, sotilaallisen ja taloudellisen painostuksen, strategisen kommunikaation sekä erilaisten ei-kineettisten operaatioiden avulla on luotu epävakaa Itä-Ukrainan alue, jota Venäjä hallitsee.

Sisäisen turvallisuuden selonteko lisää em. mainittuihin hybridivaikuttamisen keinovalikoimaan muuttoliikkeen, pakolaisten hyödyntämisen. EU-maiden johtajien kokouksessa Brysselissä 21.-22.10.2021 Valko-Venäjän pakolaispolitiikka nimettiin hybridivaikuttamiseksi.

Kesän 2021 energiakriisiin on monia syitä, mutta ei voi välttyä vaikutelmalta, että siihen on liitetty hybridivaikuttamista. Hybridioperaatioilla tavoitellaan energiasektorin hallintaa ja vaikutusvallan vahvistamista omassa etupiirissä.

Hybridivaikuttamisen torjunnassa keskeistä on tiivis poikkihallinnollinen toimintatapa sekä läheinen yhteistyö yksityisen ja kolmannen sektorin kanssa. Hybridivaikuttamista tulee torjua myös lainsäädännöllisin toimin sekä kansainvälisellä ja EU-yhteistyöllä.

Ulkoministeriössä vuonna 2018 aloittanut hybridisuurlähettiläs vahvistaa ministeriön työtä hybridikysymyksissä ja auttaa luomaan Suomen profiilia kansainvälisessä toiminnassa.

3. Kyberpuolustus

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

Kybersodankäynnissä etäisyys on merkityksetön, kun kaikki toimivat samassa globaalissa kyberympäristössä. Laitteistot, ohjelmistot, palvelut ja verkot muodostavat kybermaailman ympäristön, johon fyysinen taistelukenttä liittyy. Kyberaseet eivät perustu kineettiseen voimaan vaan älykkyyteen ja innovatiivisuuteen. Kybertaistelun voittaa se, joka käyttää huipputeknologiaa älykkäämmin ja tehokkaammin. Innovatiivisuus on kybersodankäynnissä imperatiivi – niin hyökkääjälle kuin puolustajalle.

3.1 Kansallinen kybertila/kybertoimintaympäristö tulee määritellä

Kaikkien kolmen selonteon (Ulko- ja turvallisuuspoliittinen selonteko VNS30/20, Selonteko sisäisestä turvallisuudesta VNS4/2021, Puolustusselonteko VNS 8/2021) kehittämissuunnitelmien toimeenpano edellyttää, että aluevalvontalakia (755/2000) ja siihen liittyviä säädöksiä on tarkistettava vastaamaan Suomen kybertoimintaympäristön suojaamisen tarpeita. Uudistus tarvitaan, koska meiltä 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 lähtökohtaisesti Suomen rajoille. Suomen alueellisen koskemattomuuden turvaamisessa käytetään voimakeinoja tai muita toimenpiteitä alueloukkauksen estämiseksi tai torjumiseksi.

Sisäisen turvallisuuden selonteossa esitetään määriteltäväksi kansallinen kriittinen infrastruktuuri ja selvitettävä sen suojaamiseen liittyvät lainsäädäntötarpeet. Tämä toimenpide edellyttää kansallisen kybertilan määrittelyä.

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.

3.2 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.”

Puolustusselonteon mukaan ”Puolustusvoimat on kehittänyt kybertilannekuvan muodostamista.” Selonteossa esitetään, että ”Puolustusjärjestelmän kybertilannekuvan parantaminen sekä kyberuhkien estäminen ja torjuminen edellyttävät tiedonvaihdon, toimivaltuuksien ja kansallisten yhteistyörakenteiden kehittämistä viranomaisten välillä.”

Selonteossa esitetään perustellusti, että muutosten tulee perustua viranomaisyhteistyön kehittämistarpeisiin. Ts. kansallista kybertilannetietoisuutta tulee kehittää suorituskykynäkökulmasta – kaikki hallinnolliset rajoitteet tulee voida ratkaista. Kattava kybertilannekuva on kaiken kyberpuolustuksen perusta.

3.3 Kybervoima

Kybertoimintaympäristö on yhä merkittävämpi tila, jossa vaikutetaan Suomen kansalliseen turvallisuuteen. 2020-luvun sodankäyntiin sekoittuu uusia kyberoperaatioelementtejä, joiden tavoitteena pysyttäytyä sodan kynnyksen alapuolella. Tarkoituksellisen epävakauden ylläpito ei-kineettisten operaatioiden avulla erityisesti suurvalta voi perustella fyysistä läsnäoloa ja vaikuttamista tietyllä alueella. Toimintaa perustellaan rauhanturvaamisella, tasapainon säilyttämisellä, omien etujen ja kansalaisten suojaamisella tai liittolaisten tukemisella, kaikella näennäisesti hyväksyttävällä toiminnalla. Kybertoimintaympäristön hyväksi käyttäminen soveltuu hyvin hybridisodankäyntiin ja sen eri muotoihin.

Kybervoima” (Cyber Power eli kyberkyvykkyydet valtaelementtinä) tulee maailmassa jakaantumaan niin eri valtiollisten kuin ei-valtiollisten toimijoiden kesken. Suurvalloille on mahdollista investoida laaja-alaisiin puolustuksellisiin ja hyökkäyksellisiin kyvykkyyksiin, kun taas pienet valtiot keskittyvät erikoisosaamiskykyihin.

Useat valtiot kasvattavat maa-, meri- ja ilmavoimiensa rinnalle kybervoimaa ja siihen yhdistyviä kyvykkyyksiä. Maailmassa on parhaillaan käynnissä kyberasevarustelukilpa ja sen arvioidaan kiihtyvän. Kyberkyvykkyyksiä ja niiden käyttöä määritellään eri tavoin, joten yhtenäistä määrittelyn viitekehystä on vertailuun vaikea löytää.

Harvardin Kennedy Schoolin Belfer Centerin kehittämä kansallinen kybervoimaindeksi (NCPI) mittaa 30 maan kykyjä eri indikaattoreiden avulla eri osa-alueilla kuten valvontakyky, kyberpuolustuskyky, informaatioympäristön hallinta, kybertiedustelukyky, kyberteollisuus, offensiivinen kyberkyky, kansainvälisten kybernormien ja -standardien määrittelykyky. Tässä analyysissä 10 maan kärki on 1. USA, 2. Kiina, 3. UK, 4. Venäjä, 5. Alankomaat, 6. Ranska, 7. Saksa, 8. Kanada, 9. Japani, 10. Australia. Kybervoimaindeksi mittaa niitä asioita, jotka ovat kunkin maan hallinnon omissa käsissä, ja joita se voi itse kehittää ja käyttää. Kaikkien maiden kybervoimakyvykkyydet eivät ole länsimaisen demokratiakäsitteen mukaisia.

Puolustusvoimiemme kybervoima keskittyy ensisijaisesti suojaamaan omat järjestelmänsä ja verkkonsa. Suojaamiskyky tulee mitoittaa sellaiseksi, että se mahdollisimman tehokkaasti tukee Puolustusvoimien toimintaa alueellisen koskemattomuuden turvaamiseksi ja maan puolustamiseksi.

3.4 Kyberpolitiikka ja -diplomatia

Niin kansallisessa kuin kansainvälisessä politiikassa painottuu yhä enemmän kyberasioiden poliittinen luonne (engl. Cyber Politics). Kybertoimintaympäristö itsessään ja siihen vaikuttaminen ovat voimakkaassa muutoksen tilassa, ja tätä kehitystä pyritään poliittisin keinoin ohjaamaan. Kyberturvallisuuden asiat ovat esillä yhä laajemmin ja vahvemmalla painoarvolla kansainvälisillä foorumeilla ja järjestöissä kuten ETYJ:ssä, EU:ssa, NATO:ssa, OECD:ssä ja Eurooppa-neuvostossa.

EU-johtajien kokouksessa 21.-22.10.2021 asialistalla oli myös digitalisaatio sekä kyberturvallisuus. EU-johtajat lupasivat kehittää EU:n kyberturvallisuusvalmiuksia, ja vahvistaa EU:n sitoumusta "avoimeen, vapaaseen, vakaaseen ja turvalliseen toimintaympäristöön".

Kyberturvallisuudessa valtioiden välisen luottamuksen lisääminen on keskeinen kysymys. Siihen pyritään tiivistämällä valtioiden välistä keskustelua kybertoimintaympäristöön liittyvistä kysymyksistä niin monenvälisesti, alueellisesti kuin kahdenvälisestikin. Kansainvälisillä yhteistyöfoorumeilla ja valtioiden kahdenvälisissä suhteissa vaikuttaminen on yksi keskeinen keino edistää Suomen

kyberturvallisuuden kannalta myönteisiä asioita. Ulkoministeriö koordinoi Suomen osallistumista kansainväliseen yhteistyöhön ja osallistuu aktiivisesti kybertoimintaympäristöä koskevaan kansainväliseen keskusteluun.

Kybertoimintaympäristö ja kyberturvallisuus ovat lyhyessä ajassa nousseet Suomen ulko- ja turvallisuuspolitiikan tärkeäksi osaksi. Huomionarvoisena voi myös pitää erityisen kybersuurlähettilään viran perustamista ulkoministeriöön vuonna 2014 Suomen kyberdiplomatian edistämiseksi.

Pakotteet ovat yksi EU:n kyberdiplomatian välineistön keinoista torjua ja estää EU:hun tai sen jäsenmaihin kohdistuvia haitallisia kybertoimia ja vastata niihin. EU käytti tätä välineistöä ensimmäistä kertaa heinäkuussa 2020, kun neuvosto päätti määrätä rajoittavia toimenpiteitä useista kyberhyökkäyksistä vastuussa olevia tai niihin osallistuneita kuutta henkilöä (Kiina, Venäjä) ja kolmea yhteisöä (Kiina, Pohjois-Korea, Venäjä) vastaan.

Useat valtiot ja NATO ovat rinnastaneet kyberhyökkäykset sotilaallisiin toimiin, joihin voidaan vastata kaikin mahdollisin keinoin. Kesäkuussa 2021 Nato teki linjauksen, jonka mukaan merkittävät haitalliset kybertoimet voidaan jatkossa tietyissä tapauksissa rinnastaa aseelliseen hyökkäykseen. Lokakuussa 2021 NATO-maiden puolustusministerit sopivat yleissuunnitelmasta, jossa varaudutaan Venäjän mahdolliseen aggressioon, jossa kyberoperaatiot olisivat yksi toimintamuoto.

3.5 Kyberrikollisuuden torjunta

Kyberrikolliset kehittävät jatkuvasti uusia tapoja hyökätä haluamiinsa kohteisiin. Kyberrikoksista on tullut vahva ja elinvoimainen liiketoiminnan alue. Sen arvioidaan olevan maailman kolmanneksi suurin talous. Palveluiden digitalisoituminen tuo mukanaan uudenlaisia kyberuhkia, mutta organisaatiot eivät voi ottaa taka-askeleita ja luopua verkkopalveluiden, mobiliteetin, big datan tai pilvipalveluiden tuomista hyödyistä. Digitalisaatio on synnyttänyt työtä ja kansalaisten elämää helpottavia uusia innovaatioita. Tässä tilanteessa on lähdettävä aivan uusilla tavoilla hakemaan informaatioteknologian, kyberturvallisuuden ja liiketoiminnan liittoa. Kyberuhkia vastaan toimiminen edellyttää myös uudenlaisia tapoja toimia yritysten ja julkisten toimijoiden välillä sekä myös kansainvälisessä yhteistyössä.

Sisäisen turvallisuuden selonteko toteaa, että ”Verkossa tapahtuva ja verkkoa hyödyntävä rikollisuus sekä kyberrikollisuus lisääntyvät ja kehittyvät nopeasti. Rikolliset hyödyntävät verkkoa muun muassa tiedonhankintaan ja verkostoitumiseen, sekä erilaisten vahvasti salattujen kauppapaikkojen anonymiteetin tuomiin mahdollisuuksiin.”

Tämä verkossa tapahtuva ja verkkoa hyödyntävä rikollisuuden räjähdysmäinen kasvu on ollut kolmen teknologisen innovaation konvergenssin tulosta.

1) Vuonna 2004 Yhdysvaltain laivaston tutkimuslaitos julkaisi TOR-ohjelmiston lähdekoodin vapaalla lisenssillä. TOR-verkko mahdollistaa Internetin anonyymin käytön. Nyt rikolliset saattoivat kommunikoida globaalisti vapaasti ilman kiinnijäämisen pelkoa.

2) Kryptografiaan perustuva ja lohkoketjuteknologiaa käyttävä digitaalinen virtuaalivaluutta mahdollistaa rikollisille anonyymin rahaliikenteen. Niistä tunnetuin on vuonna 2008 syntynyt Bitcoin.

3) Kyberrikolliset tarvitsevat turvallisen mobiilikommunikaation voidakseen hoitaa TOR-verkossa tapahtuneen kaupanteon käytännönjärjestelyt (esim. huume-, ase- ja ihmiskauppa). Kyberrikollisten suosituin sovellus on Wickr (2014), joka ei vaadi puhelinnumeroa tai sähköpostia, eikä sille tarvitse kertoa edes oikeaa nimeään.

Tapahtunut teknologiakonvergenssi on mahdollistanut rikollisille turvallisen toimintaympäristön. Tarvitaan osaamisen vahvistamista ja taloudellisia resursseja tämän Dark Webissä toimivan kyberrikollisuuden torjumiseksi. Jotakin onnistumisia on saatu, kuten FBI johtamassa Greenlight-operaatiossa 2021 ja Silkkitie-huumemyyntipaikan paljastumisessa 2019.

3.6 Kybertiedustelun torjunta

Sisäisen turvallisuuden selonteon mukaan ”Koronaviruspandemia on siirtänyt osin vakoilun painopistettä kyberympäristöön.” Tämä siksi, koska fyysinen liikkuminen rajojen yli hankaloitui ja koska yhteiskunta siirtyi hajautetusti verkkoon.

SUPO:n syyskuussa 2021 julkistaman kansallisen turvallisuuden katsauksen mukaan ”Suomeen kohdistuu jatkuvia kybervakoiluyrityksiä.” Itsevaltaiset valtiot pyrkivät kybervakoilun keinoin hankkimaan tietoa päätöksenteon tueksi sekä vaikuttaakseen suomalaisten päätöksentekijöiden toimintaan. Kybervakoilulla pyritään hankkimaan myös tuotekehitystietoa yrityksistä, korkeakouluista ja tutkimuslaitoksista.”

Digitaalisen kybertoimintaympäristön uusien ilmiöiden ja uhkien seuranta edellyttää uusien kyvykkyyksien luomista sotilas- ja siviilitiedustelulle. Puolustusselonteko toteaa, että sotilastiedustelua kehitetään sekä analyysi- ja tiedonhallintakykyjä vahvistetaan. Keskeistä kansallisen turvallisuuden kannalta onkin, että sotilastiedustelu toimii kiinteässä yhteistyössä siviilitiedustelun kanssa. Tarvitaan myös kansainvälistä yhteistoimintaa, sillä kybervakoilu ei tunne fyysisiä rajoja.

Hallitusohjelman mukaan tiedustelulakien mukanaan tuomat resurssitarpeet huomioidaan yhdessä sisä- ja puolustusministeriön hallinnonalojen kanssa. Hallitus antaa eduskunnalle selonteon tiedustelulakeihin liittyen vuoden 2021 loppuun mennessä. On ilmeistä, että kybertiedustelun vahvistuminen edellyttää voimavarojen vahvistamista Puolustusvoimissa ja SUPO:ssa.

4 Informaatiopuolustus - informaatiovaikuttaminen

Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko (2020) mainitsee informaatiovaikuttamisen osan globaaleja haasteita ja toteaa, että 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 halutaan hallita 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. On myös esimerkkejä muista maista, joissa vapaata tiedonvälitystä pyritään rajoittamaan.

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.” Toiminnan fokus on siis maanpuolustuksen toimintaympäristössä. Selonteko tunnistaa tarpeen yhteensovittaa eri toimintatavat viranomaisten ja muiden toimijoiden kesken ja suorituskykyjen kehittämisessä tarvitaan yhteistoimintaa kaikkien viranomaisten ja kansainvälisten kumppanien kanssa. Selonteko nostaa esiin myös toimivaltuuskysymykset.

Sisäisen turvallisuuden selonteko näkee informaatiovaikuttamisen yhteiskunnan yleisen järjestyksen ja turvallisuuden näkökulmasta. Informaatio-operaatioilla kun voidaan tuottaa ja jakaa vääristeltyä tietoa sosiaalisen median alustoilla ja siten

voidaan mobilisoida suuria ihmisjoukkoja ja lisätä yleistä levottomuutta sekä vastakkainasettelua yhteiskunnassa.

Sisäisen turvallisuuden selonteon mukaan ”Informaatiovaikuttamisen torjunnassa kansalaisten ja median tietoisuuden kasvattaminen sekä mediakasvatus ovat avainasemassa.”

VNK julkaisi 2019 oppaan informaatiovaikuttamiseen vastaamiseen. Viestijöille tarkoitettu opas tarjoaa keinoja, joilla informaatioympäristön uudenlaisiin uhkiin voidaan varautua ja jolla informaatiovaikuttamisen eri muotoja voidaan tunnistaa ja analysoida. Lisäksi opas antaa ohjeita informaatiovaikuttamiseen vastaamiseksi.

Kenen vastuulla on yhteiskuntaan kohdistuvan informaatiovaikuttamisen torjunnan kokonaiskoordinaatio? Kuinka hoidetaan normaaliaikoina esiintyvien informaatio-operaatioiden torjunta. Informaatiovaikuttamisesta kun on tullut arjen uusi normaali.

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. Lisäksi informaatio-operaatioiden havaitseminen ja arviointi edellyttävät tiedonhankinnan ja analyysitoiminnan kehittämistä.

5. 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 toteuttaa yhä kehittyneempiä kyber- ja informaatio-operaatioita, joilla on sotilaallisia, poliittisia ja taloudellisia tavoitteita. Äärimmillään niiden avulla saatuja tietoja yhteiskunnan haavoittuvuuksista hyödynnetään kriittisen infrastruktuurin sabotoimiseen, lamauttamiseen ja tuhoamiseen.

VNK julkaisi kesäkuussa 2021 periaatepäätöksen tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla. Periaatepäätöksessä on esitetty 37 poliittista linjausta, joiden toteuttamisen on arvioitu parantavan tietoturvan ja tietosuojan tasoa yhteiskunnan kriittisillä toimialoilla.

Selontekojen kyber- ja informaatiopuolustuksen kehittämisen tavoitteita on pidettävä välttämättöminä, jotta pystytään turvaamaan yhteiskunnan elintärkeitä toimintoja

normaaliaikoina, normaaliaikojen häiriötilanteissa ja poikkeusoloissa. Kehittäminen edellyttää keskitettyä suunnittelua ja johtamista sekä taloudellisia investointeja järjestelmäkehitykseen ja osaamispääoman kasvattamiseen.

Kyberturvallisuuden kehittämisohjelman (LVM 7/2021) kohdassa tehokkaat kansalliset kyberturvakyvykkyydet todetaan käynnistettävän selvitystyö, jossa arvioidaan viranomaisten toimintaedellytykset kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa, ottaen huomioon kansallisen ja kansainvälisen uhkaympäristön jatkuva kehittyminen. Työ on välttämätön kyberturvallisuuden vahvistamiseksi, tarvittavien resurssien allokoimiseksi ja lainsäädännön kehittämiseksi.

Lopuksi esimerkkinä asevoimissa tapahtuva muutos. Yhdysvaltain ilmavoimissa (USAF) on edistetty kybermaailman konvergenssia. Vuonna 2019 USAF:n esikunnassa yhdistettiin tiedustelu-, valvonta- ja kyberoperaatiot kenraaliluutnantti VeraLinn Jamiessonin johtoon. Samana vuonna jatkettiin yhdistymistä operatiivisella tasolla. Muodostettiin uusi yksikkö (16th Air Force), johon yhdistettiin kyberoperaatiot, tiedustelu- ja valvontaoperaatiot, elektroninen sodankäynti ja kryptologia. Näin ei-kineettinen suorituskyky koottu yhteen strategisella ja operatiivisella tasolla.

Työelämäprofessori, ST Martti Lehto

Jyväskylän yliopisto, Informaatioteknologian tiedekunta

martti.lehto@jyu.fi