Martti Lehto, Jyväskylän yliopisto
10.11.2021

Eduskunnan hallintovaliokunta

Asia: 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.

Digitalisaatiokehitys lisää valtiollisten ja valtiosta riippumattomien toimijoiden mahdollisuuksia toteuttaa yhä kehittyneempiä kyberoperaatioita, joilla on sotilaallisia, poliittisia ja taloudellisia tavoitteita. Äärimmillään yhteiskunnan haavoittuvuuksia hyödynnetään kyberoperaatioissa kriittisen infrastruktuurin sabotoimiseen, lamauttamiseen ja tuhoamiseen.

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.”

Digitaalisessa toimintaympäristössä kyberturvallisuuskysymykset ovat laajentuneet yhteiskunnan kaikkiin rakenteisiin. Kyberturvallisuudesta on muotoutunut useita eri poliittisia, sotilaallisia, taloudellisia, yhteiskunnallisia ja teknologisia ulottuvuuksia käsittelevä kokonaisuus.

2. POLIITTINEN JA SOTILAALLINEN ULOTTUVUUS

2.1 Kyberpolitiikka ja -diplomatia

Niin kansallisessa kuin kansainvälisessä politiikassa painottuu yhä enemmän kyberasioiden poliittinen luonne (engl. Cyber Politics). Kybertoimintaympäristö on jatkuvassa 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 ja 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. Valtioiden välistä keskustelua tulee tiivistää kybertoimintaympäristöön liittyvissä kysymyksissä 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. Tätä kuvaa kybersuurlähettilään viran perustaminen 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.

Marraskuun 2021 alussa Yhdysvallat on lisännyt israelilaisen tietotekniikkayrityksen NSO Groupin pakotelistalle yhtiön harjoittaman vahingollisen kybertoiminnan vuoksi. Perusteena yrityksen toiminta, joka on Yhdysvaltojen ulkopolitiikan linjan tai kansallisen turvallisuuden edun vastaista.

2.2 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 ylläpitoa voidaan toteuttaa kyberoperaatioiden avulla. Tämä vaikuttaminen soveltuu hyvin hybridisodankäynnin 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.

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.

Kyberkyvykkyyksiä ja niiden käyttöä määritellään eri tavoin, joten yhtenäistä viitekehystä ei ole käytössä. 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 kolmen on 1. USA, 2. Kiina, 3. UK. Kybervoimaindeksi mittaa niitä asioita, jotka ovat maan hallinnon päätettävissä, ja joita se voi itse kehittää ja käyttää. Kaikkien maiden kybervoimakyvykkyydet eivät ole länsimaisen demokratiakäsitteen mukaisia.

2.3 Kyberpuolustus

Puolustusvoimat vastaa Suomen sotilaallisesta kyberpuolustuksesta osana kansallista kyberturvallisuutta ja kybervoiman käyttöä. Puolustusvoimat varautuu laaja-alaiseen vaikuttamiseen ja kyberpuolustukseen osana kokonaisturvallisuuden mallia. Puolustusselonteon mukaan ”Kyberpuolustusta kehitetään niin, että sen avulla voidaan turvata paremmin paitsi Puolustusvoimien omat myös muut puolustuskykyyn suoraan vaikuttavat järjestelmät.”

Kybersodankäynnissä perinteiset rajat hämärtyvät, kun kaikki toimivat samassa globaalissa kyberympäristössä. Laitteistot, ohjelmistot, palvelut ja verkot muodostavat ympäristön, johon fyysinen taistelukenttä liittyy. Kyberaseet eivät perustu kineettiseen voimaan vaan älykkyyteen ja innovatiivisuuteen. Kybertaistelun voittaa se, joka käyttää huipputeknologiaa älykkäämmin ja tehokkaammin.

Kansallisella kyberpuolustuskyvykkyydellä on tulevaisuudessa yhä keskeisempi merkitys kokonaisturvallisuuden ja myös yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta. Puolustusvoimien kybersuorituskyky tulee mitoittaa sellaiseksi, että se mahdollisimman tehokkaasti tukee Puolustusvoimien kokonaissuorituskykyä.

2.4 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 selonteko tulee käsittelemään myös kyber/tietoverkkotiedustelua.

2.5 Tarvittavia toimenpiteitä sotilaallisessa ja poliittisessa ulottuvuudessa

2.5.1 Kansallinen kybertila/kybertoimintaympäristö tulee määritellä

Kaikkien kolmen selonteon (Ulko- ja turvallisuuspoliittinen selonteko 2020, Selonteko sisäisestä turvallisuudesta 2021, Puolustusselonteko 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. Suomen alueellisen koskemattomuuden valvonta määriteltyyn toimintaympäristöön. Suomen alueellisen koskemattomuuden turvaamisessa käytetään voimakeinoja tai muita toimenpiteitä alueloukkauksen estämiseksi tai torjumiseksi, jotka ovat sidottu lain määrittämään toimintaympäristöön.

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

Kansallisen kybertilan määrittely tarvitaan, jotta Suomen kybertilan koskemattomuuden valvonta ja torjunta voidaan tehokkaasti toteuttaa. Tämä tila ei ole vain teknologinen toimintaympäristö vaan merkittävällä tavalla ulko- ja turvallisuuspoliittinen toimintaympäristö.

2.5.2 Kybertilannetietoisuuden kehittäminen

EU komissio toteaa 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.”

Uusimmassa puolustuselonteossa esitetään, että ”Puolustusjärjestelmän kybertilannekuvan parantaminen sekä kyberuhkien estäminen ja torjuminen edellyttävät tiedonvaihdon, toimivaltuuksien ja kansallisten yhteistyörakenteiden kehittämistä viranomaisten välillä.”

Kybertilannekuvaympäristön rakentaminen edellyttää jaettua tilannetietoisuutta, koordinoitua ja verkostoitunutta johtamista sekä riittävää osaamista kyberturvallisuuden eri alueille. Muutosten tulee perustua viranomaisyhteistyön kehittämistarpeisiin suorituskyvyn näkökulmasta. Tilannekuva ja sen tuottama tilanneymmärrys ovat kaiken päätöksenteon perusta.

3 YHTEISKUNTA- JA KANSALAISULOTTUVUUS

Teknistaloudellinen kehitys on johtanut tuotannon, palvelujen ja koko yhteiskunnan verkostoitumiseen ja keskinäisten riippuvuuksien kasvuun. Digitalisaatio on synnyttänyt työtä ja kansalaisten elämää helpottavia uusia innovaatioita. Tietoliikenteen, tietojärjestelmien ja viestinnän toimintavarmuus onkin nykyaikaisen yhteiskunnan häiriöttömän toiminnan, turvallisuuden ja kansalaisten toimeentulon välttämätön edellytys. Kyse on myös kansalaisten luottamuksen ylläpitämisestä yhteiskunnan toimintaan.

3.1 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.

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 anonymiteettia hyödyntävien teknologisten innovaatioiden konvergenssin tulosta, joka on mahdollistanut rikollisille turvallisen toimintaympäristön. Tarvitaan osaamisen vahvistamista, taloudellisia resursseja ja yhteistyön tiivistämistä erityisesti Dark Webissä toimivan kyberrikollisuuden torjumiseksi.

4. KYBERTURVALLISUUDEN STRATEGINEN JOHTAMINEN

Yhteiskunnan turvallisuusstrategia (YTS 2017) näkee kyberturvallisuuden kiinteänä osana yhteiskunnan kokonaisturvallisuutta. Suomen kyberturvallisuuden toimintamalli perustuu tehokkaaseen ja laaja-alaiseen tiedon hankinta-, analysointi- ja keruujärjestelmään, yhteiseen ja jaettuun tilannetietoisuuteen sekä kansalliseen ja kansainväliseen yhteistoimintaan varautumisessa.

Kansallinen kyberturvallisuuden strateginen johtaminen muodostuu kahdesta kokonaisuudesta: Kyberturvallisuuden varautumisen johtaminen sekä vakavien ja laajamittaisten häiriötilanteiden hallinnan johtaminen normaali- ja poikkeusoloissa.

4.1 Kyberturvallisuuden varautumisen johtaminen

Varautumiseen yhdistyvät huoltovarmuuden ja kyberomavaraisuudesta huolehtimisen näkökulmat. Kyberturvallisuusvarautuminen kohdistuu koko yhteiskuntaan ja erityisesti kriittisen infrastruktuurimme ja elintärkeiden toimintojemme suojaamiseen kyberhyökkäyksiä vastaan. Kybervarautumiseen liittyy mm. strategiset tavoitteet, johtaminen, yhteistyörakenteet, resurssit, osaaminen ja kyvykkyydet sekä kansainvälinen yhteistoiminta.

Nykyisin eri ministeriöt ja niiden alaiset virastot toteuttavat itsenäisesti kyberturvallisuusvarautumista omilla sektoreillaan perustuen Suomen kyberturvallisuusstrategian ja kulloisenkin hallitusohjelman linjauksiin.

Perustuen vuoden 2019 kyberturvallisuusstrategiaan Valtioneuvosto nimitti 27.2.2020 ensimmäisen valtion kyberturvallisuusjohtajan sijoitettuna liikenne- ja viestintäministeriöön. Kyberturvallisuusjohtajan tehtävänä on sovittaa yhteen kyberturvallisuuden kehittämistä, suunnittelua ja varautumista. Tehtävä ja siihen liittyvät vastuut ovat parantaneet merkittävästi kansallista kyberturvallisuusvarautumista.

Valtion kyberturvallisuusjohtajan johdolla laaditussa kyberturvallisuuden kehittämisohjelmassa (2021) määritetään keskeiset toimenpiteet kyberturvallisuuden parantamiseksi koko yhteiskunnassa. Se kuvaa kyberturvallisuuden kehittämisen lyhyen ja pitkän aikavälin tavoitteita (2021–2030) ja painopistealueita. Se vastuuttaa eri hallinnonaloja kyberturvallisuuden varautumisessa ja resilienssin vahvistamisessa.

4.2 Kyberturvallisuuden häiriötilanteiden johtaminen

Kyberturvallisuuden johtaminen sisältää erityispiirteitä, jotka poikkeavat muista normaaliaikojen ja poikkeusolojen häiriötilanteista. Keskeisin tekijä on aika. Kyberhyökkäyksen valmistelu on mahdollista toteuttaa salassa ja pitkän ajan kuluessa, mutta itse hyökkäys voidaan toteuttaa erittäin lyhyessä ajassa, jolloin vastatoimenpiteiden käynnistäminen tulee aloittaa välittömästi.

Nykymallin mukaan häiriötilanteissa toimivaltainen viranomainen johtaa toimintaa ja vastaa viestinnästä. Kyberturvallisuuden häiriötilanteiden hallinnassa toimivaltainen ministeriö tai Valtioneuvoston kanslia kutsuu tarvittaessa koolle ylimääräisen valmiuspäällikkökokouksen. Samoin Valtioneuvoston tilannekeskuksen toimintaa tarvittaessa vahvennetaan, jotta voidaan muodostaa kokonaisvaltainen ja ajanmukainen tilannetietoisuus päätöksenteon tueksi. Toiminnan valmistelua ja koordinointia varten voidaan kutsua myös koolle erikseen nimitettävä kokoonpano, jota johtaa vastuunalainen valmiuspäällikkö.

Mallin vahvuus on se, että kyberhäiriötilanteen johtaminen on sulautettu olemassa oleviin häiriötilanteiden hallintajärjestelyihin ja hallinnon uudelleen järjestämisen tarve on vähäinen. Suomessa (kyber)turvallisuuden toimijat tuntevat toisensa verrattain hyvin, mikä edesauttaa tiedonvaihtoa ja yhteistyön sujumista, vaikkei yksiselitteisiä kyberturvallisuuden johtamissuhteita olisikaan tarkasti määritelty. Mallin perustana on nykyinen lainsäädäntö

Mallin heikkoutena on epävarmuus sen kyvystä reagoida riittävän nopeasti laajamittaiseen kyberhyökkäykseen tai häiriötilanteeseen, mikäli johtamismalli ja toimivaltuudet eivät ole selkeitä.

Yhteiskunnan digitalisaation lisääntyessä on välttämätöntä, että yllättäen ja nopeasti syntyvien kyberhäiriötilanteiden hallinnan edellyttämät toimenpiteet kyetään aloittamaan nopeasti. Kyberhäiriötilanteille on luonteenomaista niiden vaikuttavuuden moniulotteisuus, jonka vuoksi on välttämätöntä, että toimivaltaiselle viranomaiselle saadaan käyttöön tarvittaessa mahdollisimman laaja-alainen poikkihallinnollinen tuki. Samalla on kyettävä varmistamaan yhteiskunnan toimivuus tarkoituksenmukaisella tasolla häiriötilanteista huolimatta.

5. Yhteenveto

Hallitusohjelman mukaan kyberturvallisuuden strategista johtamista kehitetään ja kyberturvallisuuden koordinaatiota tiivistetään vastuun ollessa valtioneuvoston kanslialla. Lisäksi varmistetaan ympärivuorokautinen keskitetty tilannekuva, joka on tukena valtion virastoille, kriittisille infrastruktuurin toimijoille ja kumppaneille. Toteutuessaan tavoitteet edistävät ja vahvistavat kansallista kyberturvallisuutta.

Kyberturvallisuutta voi pitää malliesimerkkinä kokonaisturvallisuusajattelun tarpeellisuudesta, sillä kyberturvallisuudessa menestyäksemme meidän on kyettävä osallistamaan eri toimijat sekä yhteensovittamaan voimavarat ja toimintatavat mahdollisimman tehokkaasti asetettujen yhteiskunnan strategisten tavoitteiden saavuttamiseksi. Kyse on koko yhteiskunnan kyberkyvykkyyden kehittämisestä.

Vuosien 2019–2021 aikana on julkaistu useita periaatepäätöksiä, selontekoja ja suunnitelmia (ks. oheinen taulukko), joissa on ollut mukana kyberturvallisuuden kehittäminen. Kyberturvallisuuttamme on kehitetty laaja-alaisesti. Asiakirjoissa kyberturvallisuuden käsitellyissä on jonkin verran päällekkäisyyttä.

Vastuu organisaatio	**Julkaisu**
Puolustusministeriö	Kyberpuolustuksen kehittämisen strategiset linjaukset, 3.9.2019
Turvallisuuskomitea	Suomen kyberturvallisuusstrategia 3.10.2019, VN periaatepäätös
Valtiovarainministeriö	Julkisen hallinnon digitaalinen turvallisuus, 8.4.2020, VM/2020:23
Valtiovarainministeriö	Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka), 22.4.2020, VM/2020:33
Huoltovarmuuskeskus	Kyberturvallisuuden nykytila eri toimialoilla, 5.10.2020
Ulkoministeriö	Valtioneuvoston ulko- ja turvallisuuspoliittinen selonteko, 29.10.2020, VN/2020:30
Liikenne- ja viestintäministeriö	Tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla, 1.2.2021, VN periaatepäätös
Huoltovarmuuskeskus	Digitaalinen turvallisuus 2030 -ohjelma, 10.4.2021
Sisäministeriö	Valtioneuvoston selonteko sisäisestä turvallisuudesta, 20.5.2021, VN/2021:48
Liikenne- ja viestintäministeriö	Kyberturvallisuuden kehittämisohjelma, 10.6.2021, LVM/2021:7
Puolustusministeriö	Valtioneuvoston puolustusselonteko, 9.9.2021, VN/2021:78

Lisäksi suunnitelman mukaan hallitus antaa eduskunnalle selonteon tiedustelulakeihin liittyen, jossa kyber/verkkotiedustelu on todennäköisesti esillä.

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 johtamisen vahvistamiseksi, tarvittavien resurssien allokoimiseksi ja lainsäädännön kehittämiseksi.

Kansallinen kyberturvallisuuden strategisen johtamismallin tulee tukea kyberturvallisuuden kokonaisvaltaista varautumista, kehittämistä ja laajamittaisten häiriötilanteiden nopeaa hallintaa sekä sisältää riittävät toimivaltuudet, oikeusperusta. ja tilannetietoisuus.

Vaihtoehtoja ovat ainakin:

1. Nykyrakenteilla ja –prosesseilla,
2. Nykyrakenteilla selkeyttämällä vastuita, toimivaltuuksia ja päätösprosesseja,
3. Rakentamalla keskitetty kyberturvallisuuden strateginen johtamisjärjestelmä.

Em. selvitystyö antaa perusteet arvioida kyberturvallisuuden strategisen johtamisen ratkaisuvaihtoehtoja.

Kansainvälisesti kansallista kyberturvallisuutta johdetaan eri tavoin. Joitakin esimerkkejä on esitetty oheisessa taulukossa.

Maa	**Strateginen johtaminen**
Alankomaat	Turvallisuus- ja oikeusministeriö: Kansallisen kyberturvallisuuden yhteensovittaminen ja koordinaatio. Ministeriötä tukee Kyberturvallisuusneuvosto.
Australia	Strategista kyberturvallisuustoimintaa johtaa Pääministerin ja hallituksen ministeriö (=VNK). Johtaminen on keskitetty Kyberturvallisuusneuvostoon (Cyber Security Policy and Coordination Committee, CSPC).
Israel	Pääministerin toimistossa: Kansallinen kyberdirektoraatti koordinoi kyberturvallisuustoimintaa.
Saksa	BSI, Bundesamt für Sicherheit in der Informationstechnik: laaja-alaiset kyberturvallisuuspalvelut. Nationalen Cyber-Sicherheitsrat koordinoi yhteistyötä valtinhallinnon sisällä sekä yritysten kanssa.
Ranska	ANSSI, Agence Nationale de la Sécurité des Systèmes d'Information: Ranskan kansallinen kyberturvallisuusviranomainen, raportoi puolustuksen ja kansallisen turvallisuuden pääsihteerille.
Ruotsi	Keskeisin turvallisuuskoordinoija on Tietoturvallisuuden koordinaatioryhmä (SAMFI).
Singapore	Kansallinen kyberturvallisuustoimisto (CSA) toimii Pääministerin kanslian yhteydessä. Kyberturvallisuuden kriisinhallintaryhmä (CMG) johtaa laajamittaisten kyberhyökkäysten torjuntaa.
Viro	SM:n Kyberturvallisuuden kriisinhallintaryhmä (CMG) valvoo toimintaa, Talous- ja viestintäministeriö vastaa varautumisesta.
Yhdysvallat	Executive Branch Cybersecurity Coordinator, esittelyoikeus presidentille.

Kansallisen kyberturvallisuuden kehittämisen edistämiseksi ja vahvistamiseksi voisi olla tarkoituksenmukaista koota yhteen näissä eri asiakirjoissa esitetty kyberturvallisuuden linjaukset. Tällainen ”Kokonaiskyberturvallisuus” linjaisi Suomen kybermaailman poliittisia, sotilaallisia, taloudellisia, yhteiskunnallisia ja teknologisia strategisen tason tavoitteita luoden yhtenäisen kuvan kansallisesta linjasta.

Nyt esitettyjä selontekojen ja periaatepäätösten kyberturvallisuuden kehittämisen tavoitteita yhdessä kehittämisohjelman kanssa on pidettävä välttämättöminä, jotta pystytään turvaamaan yhteiskunnan elintärkeitä toimintoja normaaliaikoina, normaaliaikojen häiriötilanteissa ja poikkeusoloissa. Kehittäminen edellyttää koordinoitua suunnittelua ja johtamista sekä taloudellisia investointeja suorituskykyjen kehittämiseen ja osaamispääoman kasvattamiseen.

Työelämäprofessori, ST Martti Lehto

Jyväskylän yliopisto, Informaatioteknologian tiedekunta

martti.lehto@jyu.fi