Valiokunnan lausunto LiVL 7/2021 vp– E 3/2021 vp

Liikenne- ja viestintävaliokunta

Valtioneuvoston selvitys: Korkean edustajan ja komission yhteinen tiedonanto: EU:n kyberstrategia digitaaliselle vuosikymmenelle

Suurelle valiokunnalle

JOHDANTO

Vireilletulo

Valtioneuvoston selvitys: Korkean edustajan ja komission yhteinen tiedonanto: EU:n kyberstrategia digitaaliselle vuosikymmenelle (E 3/2021 vp): Asia on saapunut liikenne- ja viestintävaliokuntaan mahdollisia toimenpiteitä varten.

Asiantuntijat

Valiokunta on kuullut:
- EU-erityisasiantuntija Ilona Julkunen, valtioneuvoston kanslia
- neuvotteleva virkamies Olli Lehtilä, liikenne- ja viestintäministeriö
- johtaja Johanna Erkkilä, Kyberturvallisuuskeskus
- toiminnanjohtaja Mika Susi, Finnish Information Security Cluster - Kyberala ry

VALTIONEUVOSTON SELVITYS

Ehdotus

Komission ja korkean edustajan tiedonanto kyberturvallisuudesta päivittää vuonna 2013 ja 2017 julkistettuja aikaisempia EU:n kyberturvallisuusstrategioita. Tiedonannossa esitetään näkemyksiä toimista, joita tarvitaan EU:n
1) häiriönsietokyvyn, teknologisen riippumattomuuden ja johtajuuden,
2) operatiivisten valmiuksien ja
3) maailmanlaajuisen ja avoimen kybertoimintaympäristön edistämiseksi.

Kyberturvallisuus nähdään oleellisena osana Euroopan kriisinkestävyyden kehittämistä sekä vihreää ja digitaalista siirtymää. Strategiassa korostetaan sektoreiden välisten riippuvuussuhteiden merkitystä ja esitetään, että kyberturvallisuus tulee integroida osaksi EU:n rahoituskehykseen liittyviä investointeja erityisesti avainteknologioiden, kuten tekoälyn, salauksen ja kvanttilaskennan osalta.

Valmis
5.0

Valiokunnan lausunto LiVL 7/2021 vp

Valtioneuvoston kanta

Kyberturvallisuus on olennainen osa EU:n sisämarkkinoiden häiriöttömän toiminnan ja yhteiskuntavakauden sekä kansalaisten yksityisyyden turvaamista. Suomi osallistuu aktiivisesti EU:n kyberturvallisuuteen liittyvän yhteisen ulko- ja turvallisuuspolitiikan kehittämiseen ja tekee yhteistyötä EU:n kybertoimintakyvyn vahvistamiseksi. Tavoitteena on vapaa, avoin ja turvallinen kybertoimintaympäristö, jossa demokratiaperiaatetta, ihmisoikeuksia ja kansainvälistä lakia kunnioitetaan.

Suomi tukee komission ja korkean edustajan päätöstä päivittää EU:n kyberstrategia ja katsoo, että strategiassa on otettu hyvin huomioon teknologian kehityksen myötä tapahtuva kyberturvallisuuden merkityksen kasvu.

Suomi tukee kyberturvallisuusstrategian kokonaisvaltaista näkökulmaa. Operatiivisten suorituskykyjen kehittämisen osalta strategia muodostaa tarvittavan kokonaisuuden kyberuhkien ennalta ehkäisemiseksi, estämiseksi ja niihin vastaamiseksi. Muun muassa verkko- ja tietoturvaasioista vastaavien (NIS) viranomaisten, lainvalvonta- ja oikeusviranomaisten sekä kyberdiplomatiasta ja kyberpuolustuksesta vastaavien toimijoiden välisen yhteistyön ja yhteistoiminnan vahvistaminen jäsenmaissa ja EU-tasolla on kannatettavaa.

Häiriönsietokyky, teknologinen riippumattomuus ja EU:n johtoasema

Strategiassa on onnistuneesti nostettu esille verkko- ja tietoturvadirektiivin (NIS-direktiivi) keskeinen merkitys koko EU:n kyberturvallisuudelle. Suomi pitää NIS-direktiivin uudistamista tervetulleena ja yhteistä sääntelykehystä tärkeänä. Tarkemmat kannat lainsäädäntöehdotukseen otetaan asiaa koskevan U-kirjelmän yhteydessä.

On tärkeää, että EU:n yhteistä työtä 5G-verkkojen kyberturvallisuuden edistämiseksi ja yhteisen lähestymistavan luomiseksi jatketaan. Suomi pitää kannatettavana huomion keskittämistä strategisiin turvallisuustavoitteisiin (mm. riskienhallintaa koskevien lähestymistapojen yhtenäistämiseen, tiedonvaihtoon, kapasiteetin kasvattamiseen ja tuotantoketjujen resilienssiin). Myös komission tavoitetta 5G-keinovalikoiman täytäntöön panemisen seuraamiseksi vuoden 2021 aikana kannatetaan.

Suomi kannattaa komission näkemystä, että kaikkien esineiden internetiin kytkettävissä olevien laitteiden kyberturvallisuuden tulee olla sisäänrakennettua (security by design) ja että tätä periaatetta tulee soveltaa myös tekoälyssä ja kvanttilaskennassa. Suomi suhtautuu positiivisesti siihen, että internetiin kytkettävissä oleville laitteille harkitaan horisontaalista sääntelyä. Lisäksi Suomi näkee myönteisenä, että verkkotunnuspalvelujärjestelmän turvallisuutta ja diversifikaatiota kehitetään.

Suomi katsoo, että strategiassa esiin tuotu koulutuksen tarve vastaa kansallisen kyberturvallisuusstrategian tavoitteita, joita toteutetaan kyberturvallisuuden kehittämisohjelmassa. Strategian jatkokäsittelyssä tulee huomioida, että koulutusjärjestelmien ja opetuksen järjestäminen on EU:n jäsenvaltioiden toimivallassa.

Operatiivisten valmiuksien kehittäminen

Strategiassa perustettavaksi esitettävän uuden kyberyksikön tavoitteita kyberturvallisuustason kasvattamisesta ja EU-tason kyberuhkiin vastaamisesta pidetään tärkeinä. Suomi katsoo, että yksikön perustamisessa tulee kiinnittää huomiota siihen, ettei luoda päällekkäisyyksiä olemassa olevien toimijoiden kanssa. Tätä tulisi välttää myös strategiassa ehdotetun uuden tietoturvan valvomopalveluiden verkoston perustamisen osalta.

Suomi näkee komission tavoin kyberrikollisuuden torjunnan olevan avaintekijä kyberturvallisuuden varmistamisessa. Yhteistyön ja tiedonvaihdon tiivistäminen kyberturvallisuuden toimijoiden ja lainvalvonnan toimijoiden kesken on olennaista. EU:n ja kansallisten viranomaisten tulee kehittää ja vahvistaa lainvalvonnan kapasiteettia perusoikeuksia täysimääräisesti kunnioittaen. Toimintasuunnitelma lainvalvontaviranomaistoiminnan digitaalisen kapasiteetin tehostamiseksi edistäisi tätä tavoitetta.

On tärkeää mahdollistaa lainvalvonta- ja oikeusviranomaisten oikeasuhtainen tiedonsaanti kyberrikollisuuden eri muotojen ennalta estämiseksi ja niistä rikosoikeudelliseen vastuuseen saattamiseksi sekä kyberrikosten uhrien oikeuksien turvaamiseksi rikosprosessissa.

Kyberdiplomatian osalta Suomi suhtautuu rakentavasti strategiassa esiteltyihin aloitteisiin, kuten kybertiedusteluyhteistyöhön sekä kyberpakotepäätöksenteon tehostamiseen.

Suomi katsoo, että strategiassa esitetty aloite kybertiedusteluyhteistyöstä vastaavan työryhmän muodostamiseksi INTCEN:n alaisuuteen saattaisi tukea oikea-aikaisen tilannetietoisuuden muodostamissa.

Suomi suhtautuu avoimesti ehdotukseen tarkastella määräenemmistöpäätöksentekomenettelyn soveltamismahdollisuutta EU:n kyberpakotejärjestelmän yhteydessä. Myös ehdotusta EU:n kyberdiplomatiatyökalupakin soveltamista koskevien suuntaviivojen päivittämisestä säännöllisin välein pidetään kannatettavana.

Suomi suhtautuu rakentavasti strategiassa esitettyyn ajatukseen EU:n yhteisen kyberpelotetta koskevan kannan määrittelemiseen tarkemmin erityisesti kriittiseen infrastruktuuriin, demokraattisiin instituutioihin ja prosesseihin sekä toimitusketjuihin ja teollis- ja tekijänoikeuksiin kohdistuvan pahantahtoisen kybertoiminnan ennalta ehkäisemiseksi. Yhteisen lähestymistavan pohjalta EU:lla olisi nykyistä paremmat mahdollisuudet edesauttaa sääntöpohjaisuutta sekä vastuullisen valtiokäyttäytymisen ja kansainvälisen kyberyhteistyön vakiinnuttamista.

Suomi pitää kannatettavana komission ehdotusta pohtia, miten kyberdiplomatian välineistö ja SEUT-sopimuksen 42 artiklan 7 kohdan ja SEUT-sopimuksen 222 artiklan mahdollinen käyttö vaikuttavat toisiinsa.

Suomi pitää tärkeänä strategiassa mainittuja EU-puolustusyhteistyön kyberpuolustukseen ja -turvallisuuteen liittyviä aloitteita, kuten EU:n kyberpuolustuspolitiikan kehyksen päivittämistä. Suomi katsoo, että EU:n turvallisuus- ja puolustusyhteistyön strategisen arvioinnin ja ohjauksen prosessin eli ”strategisen kompassin” on tärkeää huomioida laajasti hybridi- ja kyberuhat ja uu-

det teknologiat osana EU:n turvallisuus- ja puolustusagendaa. On tärkeää, että kyberympäristö on vahvasti osa suorituskykyjen kehittämistä ja että pysyvän rakenteellisen yhteistyön sitoumusten toimeenpanossa huomioidaan jatkossa myös kyberuhkien ja tekoälyn kaltaiset poikkileikkaavat kehitykset. EU:n puolustusyhteistyön työkalut, kuten Euroopan puolustusrahasto ja puolustuksen vuosittaisen arvioinnin (CARD) johtopäätökset, tulee hyödyntää myös kyberpuolustuksen kehittämisessä. Siviili-, sotilas- ja avaruusteollisuuden synergiat ovat kannatettavia.

EU:n ja Naton välinen yhteistyö on erityisen hyödyllistä hybridi- ja kyberkysymyksissä sekä digitalisaatioon ja murrosteknologioihin, kuten tekoälyyn, liittyvissä kysymyksissä.

Globaalin ja avoimen kybertoimintaympäristön edistäminen

Suomi pitää tärkeänä, että EU toimii yhtenäisesti, määrätietoisesti ja johdonmukaisesti sääntöpohjaisen, avoimen, turvallisen ja vakaan kybertoimintaympäristön edistämiseksi niin kahdenvälisessä kuin monenvälisessä yhteistyössä ja vuoropuhelussa mm. myötävaikuttamalla etunojaisesti kybertoimintaympäristöä koskevien kansainvälisten normien ja standardien kehittämiseen EU:n perusarvojen pohjalta sekä kehittämällä yhteistyö-ja vuoropuhelumekanismeja keskeisten kolmansien kumppanimaiden ja kansainvälisten toimijoiden kanssa. Suomi suhtautuu avoimesti siihen, että EU muodostaisi yhteisen kannan kansainvälisen oikeuden soveltamisesta kyberympäristössä.

Kyberturvallisuus EU:n toimielimissä, elimissä ja virastoissa

EU:n toimielimien, elimien ja virastojen kyberturvallisuuden parantaminen on kannatettava tavoite. Suomi tukee instituutioiden välisen yhdenmukaisen lähestymistavan kehittämistä turvallisuusluokitellun tiedon ja arkaluonteisten turvallisuusluokittelemattomien tietojen käsittelyä varten. Suomi tukee myös ehdotuksia tietoturvaa koskeviksi yhteisiksi säännöiksi ja kyberturvallisuutta koskeviksi yhteisiksi säännöiksi EU:n toimielimille, elimille ja virastoille. On kuitenkin tärkeää muistaa, että avoimuuden periaate on kirjattu perussopimuksiin ja oikeus tutustua asiakirjoihin tunnustetaan perusoikeudeksi perusoikeuskirjassa. Avoimuus ja turvallisuuskysymykset voidaan sovittaa yhteen.

Suomi katsoo myös, että covid-19-pandemian aikaisia kokemuksia digitaalisten välineiden hyödyntämisestä kriisi- ja häiriötilanteissa sekä laajemminkin tulisi tarkastella myönteisessä hengessä, mukaan lukien etätyöskentelyyn tarvittavan teknisen välineistön kehittäminen sekä turvallisen kokousympäristön asettamien vaatimusten arvioiminen.

Suomen kantoja tiedonannossa mainittuihin eri aloitteisiin täsmennetään kunkin toimenpide-ehdotuksen antamisen yhteydessä.

VALIOKUNNAN PERUSTELUT

Asiantuntijakuulemisessa EU:n kyberstrategian sisältöä on pidetty varsin onnistuneena ja Suomen kantaa perusteltuna. Kuulemisessa on korostettu kyberturvallisuuden kasvavaa elinkeinopoliittista roolia. Strategiassa on otettu hyvin huomioon teknologian kehityksen myötä tapahtuva

kyberturvallisuuden merkityksen kasvu. Asiantuntijakuulemisessa on kuitenkin katsottu, että huomiota tulee kiinnittää myös kyberturvallisuuden perusasioihin, kuten matkapuhelinverkkojen perustason tietoturvan varmistamiseen.

Uudet toimijat

Strategiassa perustettavaksi esitettävän uuden yhteisen kyberturvallisuusyksikön tavoitteet kyberturvallisuustason kasvattamisesta ja EU-tason kyberuhkiin vastaamisesta ovat tärkeitä. Valiokunta korostaa, että mahdollisen uuden yksikön perustamisessa tulee kiinnittää huomiota siihen, ettei luoda päällekkäisyyksiä olemassa olevien toimijoiden kanssa.

Strategiassa ehdotetaan perustettavaksi myös uusi tietoturvan valvomopalveluiden verkosto. On tärkeää, ettei perustettavaksi ehdotetulla verkostolla luoda päällekkäisyyksiä olemassa olevien operatiivisten tiedonvaihtokanavien kanssa. Tietoturvan valvomopalveluiden verkostolla ei myöskään pitäisi luoda päällekkäisyyksiä strategiassa perustettavaksi esitetyn uuden kyberyksikön kanssa.

Esineiden internet

Valiokunta pitää kannatettavana tavoitetta internetiin kytkettyjen laitteiden ja niihin liittyvien palveluiden kyberturvallisuuden parantamiseksi. Kaikkien esineiden internetiin kytkettävissä olevien laitteiden kyberturvallisuuden tulee olla strategiassa esitetyllä tavalla sisäänrakennettua (security by design). Kyberturvallisuuden sertifioinnilla voidaan lisätä tuotteiden ja palveluiden turvallisuutta. On kuitenkin tärkeää, että sertifiointitoiminnalla ei aiheutettaisi suomalaisille yrityksille ylimääräistä, kilpailukykyä haittaavaa taakkaa.

5G-verkon kyberturvallisuus

On tärkeää jatkaa EU-tason yhteistyötä 5G-verkkojen kyberturvallisuuden edistämiseksi ja yhteisen lähestymistavan kehittämiseksi. Vaikka 5G-verkkojen kyberturvallisuus sivuaa kunkin jäsenvaltion vastuulla olevaa kansallista turvallisuutta, voidaan EU:n tasolla luoda yhteinen pohja viestintäverkkojen turvallisuudelle, joka tukee kansallisia ratkaisuja.

Kriittisten toimialojen kyberturvallisuus ja sietokyky

Valiokunta korostaa kriittisten toimialojen suojaamisen merkitystä ja toteaa, että verkko- ja tietoturvadirektiivin (NIS) päivittämisen osalta on tarpeellista panostaa kriittisten toimialojen kyberturvallisuuteen. Asiantuntijakuulemisessa valiokunnan huomiota on kiinnitetty siihen, että sääntelyn tuottamien velvoitteiden tulee olla huolelliseen riskianalyysiin perustuvia ja kustannustehokkaisiin investointeihin kannustavia. Näin voidaan luoda hyvä perusta kokonaisvaltaisen kyberturvallisuuden parantamiselle.

VALIOKUNNAN LAUSUNTO

Liikenne- ja viestintävaliokunta ilmoittaa,

että se yhtyy asiassa edellä esitetyin täsmennyksin valtioneuvoston kantaan.

Helsingissä 4.3.2021

Asian ratkaisevaan käsittelyyn valiokunnassa ovat ottaneet osaa

puheenjohtaja Suna Kymäläinen sd
varapuheenjohtaja Ari Torniainen kesk
jäsen Pekka Aittakumpu kesk
jäsen Sandra Bergqvist r
jäsen Seppo Eskelinen sd
jäsen Janne Heikkinen kok
jäsen Juho Kautto vas
jäsen Jouni Kotiaho ps
jäsen Johan Kvarnström sd
jäsen Joonas Könttä kesk
jäsen Sheikki Laakso ps
jäsen Jenni Pitko vihr
jäsen Mirka Soinikoski vihr
jäsen Kari Tolvanen kok
jäsen Paula Werning sd

Valiokunnan sihteerinä on toiminut

valiokuntaneuvos Mika Boedeker