U 20/2023 vp

Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksista Euroopan parlamentin ja neuvoston asetuksiksi (kybersolidaarisuussäädös ja kyberturvallisuusasetuksen muuttaminen)

Perustuslain 96 §:n 2 momentin perusteella lähetetään eduskunnalle komission 18 päivänä huhtikuuta 2023 tekemät ehdotukset Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten sekä Euroopan parlamentin ja neuvoston asetukseksi asetuksen (EU) 2019/881 muuttamisesta tietoturvapalvelujen osalta sekä näistä laadittu muistio.

Helsingissä 6.7.2023

Liikenne- ja viestintäministeri Lulu Ranne

Erityisasiantuntija Emma Hokkanen

LIIKENNE- JA VIESTINTÄMINISTERIÖ | MUISTIO | EU/688/2023

6.7.2023

KOMISSION EHDOTUKSET EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSIKSI (KYBERSOLIDAARISUUSASETUS JA KYBERTURVALLISUUSASETUKSEN MUUTTAMINEN)

1 Tausta

Euroopan komissio teki 18.4.2023 ehdotuksen (COM(2023) 209 final) Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten (kybersolidaarisuussäädös). Uuden sääntelyn lisäksi asetuksella muutettaisiin asetusta (EU) 2021/694 (Digitaalinen Eurooppa -ohjelma). Ehdotuksen taustalla on kyberturvallisuuteen liittyvä kehitys, jossa kyberhyökkäysten määrä on kasvanut ja digitaalisten teknologioiden yleistyminen yhteiskunnissa lisäävät altistumista kyberturvallisuuden häiriöille ja niiden mahdollisille valtioiden rajat ylittäville vaikutuksille. Merkittäviä häiriöitä aiheuttavan häiriötilanteen uhka kriittisille infrastruktuureille vaatii parempaa varautumista ja yhteistyötä kaikilla EU:n kyberturvallisuusekosysteemin tasoilla. EU on tukenut digitalisaatiota Digitaalinen Eurooppa -ohjelman rahoituksella. Yksi ohjelman viidestä erityistavoitteesta on kyberturvallisuus ja luottamus.

Komissio teki 18.4.2023 myös ehdotuksen (COM(2023) 208 final) Euroopan parlamentin ja neuvoston asetukseksi asetuksen (EU) 2019/881 muuttamisesta tietoturvapalvelujen osalta (kyberturvallisuusasetuksen muuttaminen). Ehdotus täydentää kybersolidaarisuussäädösehdotusta, jossa esitetään, että kyberturvallisuusreservin palveluntarjoajien valinnassa tulisi ottaa huomioon luotettavien palveluntarjoajien sertifioinnit.

Alustavien tietojen mukaan kyberturvallisuusasetuksen muutosehdotuksia käsiteltäisiin samanaikaisesti kybersolidaarisuussäädösehdotuksen kanssa.

2 Ehdotuksen tavoite

Kybersolidaarisuussäädösehdotuksen yleisenä tavoitteena on vahvistaa EU:n yhteistä kyberhäiriöiden havainnointia, tilannekuvaa sekä kyvykkyyttä vastata kyberhäiriöihin. Toisena tavoitteena on vahvistaa kriittisten toimijoiden valmiuksia koko EU:ssa ja vahvistaa solidaarisuutta kehittämällä yhteisiä toimintavalmiuksia merkittävien tai laajamittaisten kyberturvallisuuspoikkeamien varalle, mukaan lukien tarjoamalla kyberhäiriötilanteiden hallintaan liittyvää tukea kolmansille maille. Tavoitteena on myös edistää Euroopan teknologista riippumattomuutta kyberturvallisuuden alalla. Lisäksi tavoitteena on parantaa kriisinsietokykyä ja edistää tehokasta toimintaa kyberhäiriöiden hallinnassa luomalla arviointimekanismi, jonka avulla arvioidaan merkittäviä tai laajamittaisia vaaratilanteita ja niiden hallinnasta saatuja kokemuksia.

Kyberturvallisuusasetukseen ehdotetuilla muutoksilla lisättäisiin tietoturvapalveluntarjoajat (*managed security services provider*) kyberturvallisuusasetuksen soveltamisalaan. Keväällä 2022 annetuissa neuvoston päätelmissä kehotetaan unionia parantamaan kyberturvallisuuden kokonaistasoa esimerkiksi helpottamalla tietoturvapalvelutarjoajien syntymistä todeten, että tällaisten palveluiden saatavuuden edistämisen tulisi olla unionin teollisuuspolitiikassa kybertur-

vallisuudessa etusijalla. Ehdotuksen perustelujen mukaan komissio näkee, että tietoturvapalvelutarjoajien sertifiointi voi olla tehokas keino lisätä luottamusta näiden palvelujen laatuun ja siten helpottaa luotetun eurooppalaisen kyberturvallisuuspalvelualan syntymistä. Kyberturvallisuusasetukseen ehdotetuilla muutoksilla tietoturvapalvelutarjoajista tarkoitetaan kybersolidaarisuusasetusehdotuksen 16 artiklassa mainittuja luotettuja palveluntarjoajia (*trusted providers*).

Komissio huomauttaa, että osassa jäsenvaltioissa on jo otettu käyttöön tietoturvapalvelutarjoajia koskevia sertifiointijärjestelmiä. Ehdotuksella sertifiointijärjestelmistä kyseisille palveluille pyritään estämään palveluiden pirstaloituminen jäsenmaissa.

3 Ehdotuksen pääasiallinen sisältö

3.1 Kybersolidaarisuussäädösehdotuksen pääasiallinen sisältö

Ehdotuksessa esitetään yleiseurooppalaisen turvaoperaatiokeskusten infrastruktuurin (Security Operations Center, SOC) perustamista ja niiden yhteistyöinfrastruktuurin käyttöönottoa (European Cyber Shield, eurooppalainen kybersuojakilpi) unionin yhteisten havainnointi- ja tilannekuvavalmiuksien tehostamiseksi ja vahvistamiseksi.

Lisäksi ehdotuksessa esitetään kyberhätämekanismin ja luotettavista yksityisen sektorin palveluntarjoajista koostuvan kyberturvallisuusreservin perustamista jäsenvaltioiden tukemiseksi merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa, niihin vastaamisessa ja niistä välittömästi toipumisessa.

Ehdotuksessa myös esitetään kyberturvallisuuspoikkeamien arviointimekanismin perustamista tiettyjen merkittävien tai laajamittaisten poikkeamien tarkastelua ja arviointia varten. Eurooppalaista kybersuojakilpeä, kyberhätämekanismia sekä kyberturvallisuusreserviä esitetään tuettavaksi Digitaalinen Eurooppa-rahoituksesta, jota tällä säädöksellä esitetään muutettavaksi ehdotuksen toimien toteuttamiseksi.

3.1.1 Yleiset säännökset

Komission ehdotuksen mukaan säädöksellä vahvistetaan unionin valmiuksia havaita, varautua ja reagoida kyberturvallisuusuhkiin ja –häiriöihin.

Ehdotuksella ei rajoiteta jäsenvaltioiden ensisijaista vastuuta kansallisesta turvallisuudesta, yleisestä turvallisuudesta sekä rikosten ehkäisemisestä, tutkimisesta, paljastamisesta ja syytteeseenpanosta.

3.1.2 Eurooppalaisen kybersuojakilven perustaminen

Ehdotuksen nojalla perustettaisiin yhteiseurooppalainen turvaoperaatiokeskusten infrastruktuuri (eurooppalainen kybersuojakilpi), joka kehittäisi tapoja havainnoida analysoida ja prosessoida tietoa kyberuhista ja kyberhäiriöistä unionissa. Suojakilpi koostuisi kansallisista turvaoperaatiokeskuksista (SOC) sekä rajojen yli toimivista SOC-yhteenliittymistä. Kybersuojakilven kyvykkyyksien rakentamista tuettaisiin Digitaalinen Eurooppa-ohjelmasta ja sen kolmannesta erityistavoitteesta (kyberturvallisuus ja luottamus).

Eurooppalaisen kybersuojakilven tulisi koota ja jakaa eri lähteistä peräisin olevia kyberuhkatietoja rajojen yli toimivista SOC-yhteenliittymissä sekä tuottaa korkealaatuista ja käyttökelpoista kyberuhkatietoa käyttämällä kehittyneitä teknologioita, kuten tekoälyä ja data-analytiikkateknologiaa. Lisäksi suojakilven tulisi nopeuttaa kyberuhkien havaitsemista sekä tarjota palveluja

EU:n kyberturvallisuusyhteisölle, kuten osallistumista kehittyneiden tekoälyn ja data-analytiikan työkalujen kehittämiseen.

Osallistuakseen eurooppalaiseen kybersuojakilpeen, jokaisen jäsenvaltion tulisi nimetä vähintään yksi julkinen elin, joka toimisi kansallisena turvaoperaatiokeskuksena (SOC). Kansallisella SOC-toimijalla olisi oltava valmiudet toimia yhteyspisteenä muille kansallisille julkisille ja yksityisille organisaatioille kyberuhkiin liittyvän tiedon kerääjänä ja analysoijana. SOC-toimijalla tulisi olla kyvykkyys osallistua myös rajojen yli toimivaan, kansallisista SOC-toiminnoista koostuvaan SOC-yhteenliittymään. Kansallisen SOC-toiminnon tulisi hyödyntää kehittyneitä teknologioita, jotka pystyvät havaitsemaan ja analysoimaan kyberturvallisuusuhkiin ja -häiriöihin liittyviä tietoja. Kansallinen SOC-toiminto voisi osallistua kyberturvallisuuden eurooppalaisen osaamiskeskuksen(ECCC) yhteishankintoihin, joiden kautta yllämainittuja työkaluja voidaan hankkia komission 50 % rahoitustuella.

Vähintään kolmea jäsenmaata edustavat kansalliset SOC-toiminnot voivat perustaa yhdessä rajojen yli toimivan SOC-yhteenliittymän. Myös yhteenliittymälle voidaan myöntää 50-75% rahoitustukea yhteishankintoihin ja käyttökustannuksiin, joilla yhteenliittymävoi hankkia käyttöönsä kehittyneitä havainnointi- ja analysointityökaluja. Ennen hankintamenettelyn aloittamista ECCC:n ja yhteenliittymän tulee tehdä isännöinti- ja käyttösopimus, jossa määritetään ehtoja työkalujen käytölle.

Yhteishankintoihin osallistumisen edellytyksenä kansallisille SOC-toimijoille on sitoutuminen rajojen yli toimivaan SOC-yhteenliittymään kahden vuoden kuluessa siitä päivästä, jona työkalut on hankittu tai avustusrahoitusta alettu saada riippuen siitä, kumpi näistä tapahtuu aikaisemmin.

ECCC:n ja yhteenliittymän välisen sopimuksen lisäksi myös yhteenliittymän jäsenten tulee tehdä keskinäinen sopimus, jossa määritellään ja vahvistetaan yhteenliittymän sisäiset järjestelyt isännöinti- ja käyttösopimuksen täytäntöön panemiseksi. Keskinäisessä yhteenliittymäsopimuksessa osallistujien tulisi sitoutua jakamaan yhteenliittymän sisällä merkittävä määrä tietoa muun muassa kyberuhista, läheltä piti-tilanteista, haavoittuvuuksista, uhkatoimijoista, varoituksista sekä kyberhyökkäysten havainnointityökalujen konfiguroinnista silloin kun kyseisten tietojen vaihto tähtää kyberhäiriöiden ehkäisemiseen, havaitsemiseen, niihin vastaamiseen tai niistä palautumiseen. Vaihtoehtoisesti sopimuksessa tulisi sitoutua jakamaan kyseisiä tietoja, kun tiedonvaihto parantaa kyberturvallisuutta esimerkiksi rajoittamalla tai estämällä uhkien leviämistä, tukemalla erilaisia puolustusvalmiuksia, haavoittuvuuksia korjaamalla tai niiden paljastamisella.

Keskinäisessä sopimuksessa yhteenliittymän jäsenten tulisi määritellä ehdot, missä tilanteissa yhteenliittymän jäsenet vaihtavat keskenään edellä mainittuja tietoa. Lisäksi sopimuksessa tulisi luoda yhteenliittymälle sellainen hallintomalli, joka kannustaa osapuolia jakamaan tietoja sekä määritellä tavoitteet, joilla edistetään kehittyneiden tekoälyn ja data-analytiikan työkalujen kehittämistä.

Myös rajojen yli toimivien SOC-yhteenliittymien tulisi tehdä keskenään yhteistyösopimuksia, joissa täsmennetään periaatteet eri yhteenliittymien väliselle tiedonvaihdolle. Tilanteessa, jossa rajat ylittävät SOC-yhteenliittymät saavat tietoja mahdollisesta tai meneillään olevasta laajamittaisesta kyberhäiriöstä, tulisi niiden viipymättä toimittaa asiaankuuluvia tietoja myös CyCLONe- ja CSIRT-verkostolle sekä komissiolle ottaen huomioon niiden NIS2-direktiivin mukaiset kriisinhallintatehtävät. CSIRT-verkosto (*Computer Security Incident Response Teams*) ja

CyCLONe-verkosto (*European Cyber Crisis Liaison Organisation Network*) ovat EU:n laajuisia jo olemassa olevia kyberturvallisuuden yhteistyö- ja tiedonvaihtoverkostoja. Suomi osallistuu molempien verkostojen toimintaan.

Komissio voisi täytäntöönpanosäädöksillä vahvistaa CyCLONe- ja CSIRT-verkostolle sekä komissiolle luovutettaviin tietoihin liittyvät menettelytavat, rajojen yli toimivien SOC-yhteenliittymien yhteentoimivuuden vaatimukset sekä SOC-toimintojen turvallisuuden teknisiä vaatimuksia.

3.1.3 Kyberhätätilanteiden mekanismin ja kyberturvallisuusreservin perustaminen

Ehdotuksessa esitetään kyberhätätilanteiden mekanismin perustamista (Cyber Emergency Mechanism).

Mekanismilla toteutettaisiin varautumis- ja valmiustoimia, merkittäviin ja laajamittaisiin kyberhäiriötilanteisiin reagointitoimenpiteitä sekä keskinäistä avunantoa koskevia toimia, joissa jäsenvaltion kansallisilta viranomaisilta annetaan apua toiselle jäsenvaltiolle, erityisesti NIS2-direktiivin 11 artiklan 3 kohdan f alakohdan mukaisesti CSIRT-verkoston kautta.

Osana kyberhätätilanteiden mekanismia voitaisiin toteuttaa myös varautumisen koordinoitua testausta. Varautumistestauksien toteuttamiseksi komissio määrittelee NIS2-direktiivin liitteessä I luetelluista toimialoista sellaiset toimialat, joille voitaisiin suorittaa koordinoitu varautumistestaus. Varautumistestausten sisältöä, toteuttamistahoa tai muita menettelyitä ei ole kuvattu ehdotuksessa tarkemmin. Ehdotuksen mukaan NIS-yhteistyöryhmä laatisi yhteistyössä komission, Euroopan kyberturvallisuusvirasto ENISAn ja korkean edustajan kanssa yhteisiä riskiskenaarioita sekä metodologiaa koordinoituja testauksia varten.

Osana kyberhätätilanteiden mekanismia ehdotuksessa esitetään myös EU:n kyberturvallisuusreservin perustamista. Reservi koostuisi luotettavista palveluntarjoajista (*trusted providers)* ja se antaisi tukea merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin reagoimisessa tai tällaisista poikkeamista toipumisesta jäsenvaltioiden pyynnöstä. Jäsenvaltioiden kriittisten tai erittäin kriittisten alojen toimijat sekä unionin instituutiot, virastot ja toimielimet voisivat saada reservin palveluita vastatakseen organisaatioon kohdistuneisiin merkittäviin tai laajamittaisiin kyberpoikkeamiin, saadakseen tukea kyseisiin häiriöihin reagoimisessa tai niistä toipumisessa. Palvelupyyntöjä voisivat esittää jäsenvaltion NIS2-direktiivin mukainen kyberkriisinhallintaviranomainen sekä CSIRT-toimija. Tukipyynnöt tulisi toimittaa komissiolle ja ENISAlle NIS2-direktiivin mukaisen keskitetyn yhteyspisteen kautta. Saadakseen tukea EU:n kyberturvallisuusreservistä myös tukea pyytävien tahojen on toteutettava toimenpiteitä, joilla lievennetään sen poikkeaman vaikutuksia, johon tukea pyydetään.

Reserville kohdistettuihin pyyntöihin tulisi sisällyttää asianmukaiset tiedot häiriön kohteena olevasta toimijasta, vaaratilanteen mahdollisista vaikutuksista sekä pyydetyn tuen suunnitellusta käytöstä, mukaan lukien tiedot arvioiduista tarpeista, tiedot toimista, jotka on jo toteutettu vaaratilanteen lieventämiseksi sekä tiedot muista asianomaisen yhteisön käytettävissä olevista tukimuodoista, mukaan lukien vaaratilanteiden torjuntaa koskevat sopimusjärjestelyt sekä vakuutussopimukset, jotka mahdollisesti kattavat tällaisen vaaratilanteen korvaamisen. ENISA laatisi yhteistyössä komission ja NIS-yhteistyöryhmän kanssa mallin tukipyyntöjen jättämiselle. Jäsenvaltioiden on ilmoitettava CSIRT-verkostolle ja tarvittaessa EU-CyCLONelle pyynnöistään.

Komissio arvioisi ENISAn tuella EU:n kyberturvallisuusreserville osoitetut tukipyynnöt ja vastaus pyyntöön olisi toimitettava viipymättä. Tukipyyntöjä voitaisiin priorisoida huomioiden kyberturvallisuuspoikkeaman vakavuus, mahdolliset vaikutukset asianomaisiin jäsenvaltioihin tai käyttäjiin, joita asia koskee, häiriön mahdollinen rajat ylittävä luonne sekä toimija, johon häiriö vaikuttaa asettaen NIS2-direktiivissä tarkoitetut keskeiset toimijat etusijalle.

Reservin täytäntöönpanon vastuu olisi komissiolla. Komissio määrittelisi reservin painopisteet, valvoisi sen täytäntöönpanoa ja varmistaisi mahdolliset linkitykset muihin tämän asetuksen mukaisiin tukitoimiin sekä muihin unionin toimiin ja ohjelmiin. Komissio voisi antaa EU:n kyberturvallisuusreservin toiminnan ja hallinnoinnin kokonaan tai osittain myös ENISAn tehtäväksi. Tukeakseen komissiota EU:n kyberturvallisuusreservin perustamisessa ENISA laatisi kartoituksen tarvittavista palveluista.

Palveluiden käyttäjien olisi kuukauden kuluessa tukitoimenpiteen päättymisestä toimitettava komissiolle ja ENISAlle yhteenveto tarjotusta palvelusta, saavutetuista tuloksista, kokemuksista ja opeista. Komissio raportoisi säännöllisesti NIS-yhteistyöryhmälle tuen käytöstä ja saavutetuista tuloksista. Komissio voisi täytäntöönpanosäädöksillä täsmentää EU:n kyberturvallisuusreservin palveluiden järjestämistä sekä EU:n kyberturvallisuusreservistä annettavien palvelujen määritelmiä.

Ehdotuksessa huomioidaan, että mikäli kyberturvallisuuspoikkeamat ovat EU:n pelastuspalvelumekanismin mukaisia katastrofeja tai johtavat niihin, annettavassa tuessa tulee huomioida pelastuspalvelumekanismin mukaiset menettelyt.

Lisäksi ehdotuksessa esitetään, että kyberhätätilanteiden mekanismin avulla voitaisiin täydentää yhteisen ulko- ja turvallisuuspolitiikan sekä yhteisen turvallisuus- ja puolustuspolitiikan yhteydessä annettavaa apua, myös nopean kybertoiminnan joukkojen (Cyber Rapid Response Teams) kautta. Nopean kybertoiminnan joukkojen toiminta perustuu jäsenvaltioiden vapaaehtoisuuteen, johon osallistuu vain osa jäsenmaista pääosin puolustushallinnon alalta. Suomi on mukana tarkkailijajäsenenä. Lisäksi, mekanismilla annettu jäsenvaltioiden välinen tuki voisi olla Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohdan mukaisesti antamaa apua. Kyberhätätilamekanismin mukainen tuki voisi olla myös osa unionin ja jäsenvaltioiden yhteistä toimintaa Euroopan unionin toiminnasta tehdyn sopimuksen 222 artiklassa tarkoitetuissa tilanteissa.

EU:n kyberturvallisuusreservin perustamista koskevissa järjestelyissä hankintamenettelyille annetaan tiettyjä vaatimuksia. Hankinnoissa olisi esimerkiksi varmistettava, että EU:n kyberturvallisuusreservi sisältää palveluja, joita voidaan käyttää kaikissa jäsenvaltioissa, ottaen erityisesti huomioon tällaisten palvelujen tarjoamista koskevat kansalliset vaatimukset, kuten palveluiden sertifiointi. Hankinnoissa tulisi myös huolehtia unionin ja sen jäsenvaltioiden keskeisten turvallisuusetujen suojaamisesta sekä varmistettava, että reservi tuo lisäarvoa edistämällä Digitaalinen Eurooppa-asetuksen 3 artiklassa asetettujen tavoitteiden saavuttamista.

Hankkiessaan palveluja EU:n kyberturvallisuusreserviä varten hankintaviranomaisen olisi huomioitava valintaperusteina palveluntarjoajan ammatillinen osaaminen, luotettavuus ja pätevyys, palveluntarjoajan riittävä kokemus vastaavien palvelujen tarjoamisesta asiaankuuluville kansallisille viranomaisille tai kriittisillä tai erittäin kriittisillä aloilla toimiville yksiköille, kyvykkyys tarjota palvelu lyhyessä ajassa sekä sen jäsenvaltion paikallisella kielellä, jossa se voi tarjota palvelun. Palveluntarjoajalla olisi myös oltava soveltuvat tekniset laitteet palvelun toteuttamiseksi.

Turvallisuusvaatimusten osalta palveluntarjoajalta vaadittaisiin asianmukaiset turvallisuusselvitykset vähintään palvelujen käyttöönottoon tarkoitetusta henkilöstöstä ja tietojärjestelmiensä asianmukaisesta suojaustasosta sekä riittävät toimenpiteet tietojen suojaamiseksi ja turvallisuuden varmistamiseksi palvelun toteuttamiseksi. Lisäksi ehdotuksessa todetaan, että palveluntarjoaja olisi sertifioitava kyberturvallisuusasetuksen (EU) 2019/881 mukaisesti, mikäli EU-sertifiointijärjestelmä on käytössä kyseisille tietoturvapalvelun tarjoajille.

Myös kolmannet maat ja niiden toimivaltaiset viranomaiset, kuten CSIRT-toimijat ja kyberkriisinhallintaviranomaiset voisivat pyytää tukea EU:n kyberturvallisuusreserviltä, jos tämä on erikseen määritelty niiden DEP-ohjelmaan liittyvissä assosiaatiosopimuksissa. Ennen tuen saamista kolmansien maiden olisi toimitettava komissiolle ja korkealle edustajalle tietoja muun muassa niiden kyberresilienssistä ja riskienhallintavalmiuksista, sekä tiedot kansallisista toimenpiteistä, jotka on toteutettu merkittäviin tai laajamittaisiin kyberturvallisuuspoikkeamiin varautumiseksi.

3.1.4 Kyberhäiriöiden jälkitarkastelumekanismi

Ehdotuksessa esitetään, että ENISA voisi tarkastella ja arvioida komission, EU-CyCLONe-verkoston tai CSIRT-verkoston pyynnöstä tiettyyn merkittävään tai laajamittaiseen kyberturvallisuushäiriöön liittyviä uhkia, haavoittuvuuksia ja häiriöön liittyviä hallintatoimia. Tarkastelun lopputuloksena ENISAn tulisi toimittaa CSIRT-verkostolle, EU-CyCLONe-verkostolle ja komissiolle poikkeaman jälkitarkasteluarviointiraportti. Tarkasteluraportilla tuettaisiin kyseisiä toimijoita erityisesti NIS2-direktiivissä säädettyjen tehtävien suorittamisessa. Komissio voisi jakaa raportin tarvittaessa korkealle edustajalle.

Tarkasteluraportin laatimiseksi ENISAn tulisi tehdä yhteistyötä kaikkien asiaankuuluvien sidosryhmien kanssa, mukaan lukien jäsenvaltioiden, komission, muiden asiaankuuluvien EU:n toimielinten, elinten ja virastojen, tietoturvapalveluntarjoajien ja kyberturvallisuuspalvelujen käyttäjien edustajat. ENISAn olisi tarvittaessa tehtävä yhteistyötä myös sellaisten muiden tahojen kanssa, joihin merkittävät tai laajamittaiset kyberturvallisuuspoikkeamat vaikuttavat. Arvioinnin tueksi ENISA voisi kuulla myös muita sidosryhmiä.

ENISAn jälkitarkasteluraportissa tulisi tarkastella ja analysoida kyberturvallisuushäiriötä, siihen johtaneita syitä, haavoittuvuuksia sekä häiriöstä saatuja kokemuksia. Luottamuksellisia tietoja olisi suojattava unionin tai kansallisen lainsäädännön mukaisesti. Raportissa voitaisiin esittää tarvittaessa suosituksia unionin kyberturvallisuuden parantamiseksi. Osa raportista olisi mahdollisuuksien mukaan asetettava julkisesti saataville. Tämä versio saisi sisältää vain julkista tietoa.

3.1.5 Loppusäännökset

Loppusäännöksissä ehdotetaan Digitaalinen Eurooppa-rahoitusohjelmaa koskevaan sääntelyyn (EU) 2021/694 muutoksia. Ehdotuksessa esitetään 6 artiklan täydentämistä, siten että eurooppalainen kybersuojakilpi ja kyberhätätilanteiden mekanismi tulisi osaksi DEP-ohjelmaa. Lisäksi artiklaa muutettaisiin niin, että erityistavoitteen 3 (kyberturvallisuus ja luottamus) toimenpiteiden toimeenpanon vastuu olisi pääasiallisesti kyberturvallisuuden eurooppalaisella osaamiskeskuksella (ECCC), mutta kyberturvallisuusreservin toimeenpanon vastuu olisi komissiolla ja ENISAlla.

Ehdotuksessa esitetään 9 artiklan rahoituspuitteisiin muutoksia, niin että erityistavoitteelle 2 (tekoäly) allokoitua ohjeellista määrää vähennettäisiin 285 000 000 eurolla, erityistavoitteen 3

(kyberturvallisuus ja luottamus) määrää 20 000 000 eurolla ja erityistavoitteen 4 (edistynyt digitaalinen osaaminen) määrää 95 000 000 eurolla.

Lisäksi ehdotuksessa esitetään tarkennuksia erityistavoitteen 3 ylijäämän käytön osalta seuraavana vuonna sekä siihen, että kyberreservin osalta ENISA ja komissio voisivat toimia hankkivana osapuolena. Tuen hakumenettelyjen osalta muutettaisiin 14 artiklaa niin, että solidaarisuusaloitteen mukaisille kansallisille SOC-toimijoille, rajojen yli toimiville SOC-yhteenliittymille, ja hätätilanteiden mekanismin palveluiden käyttöön voitaisiin myöntää avustuksia ilman hakukuulutusta.

Komission tulee tarkastella asetuksen toimivuutta neljän vuoden kuluttua asetuksen soveltamisen alkamisesta. Asetus astuisi voimaan 20. päivänä sen julkaisusta Euroopan virallisessa lehdessä.

3.2 Ehdotus kyberturvallisuusasetuksen muuttamisesta

Ehdotus kyberturvallisuusasetuksen muuttamiseksi sisältää useita teknisiä muutoksia, joilla lisättäisiin tietoturvapalveluntarjoajat kyberturvallisuusasetuksen ((EU) 2019/881) ja sen velvoitteiden piiriin. Lisäksi ehdotus sisältää uuden artiklan, jossa määritellään tietoturvapalveluntarjoajien eurooppalaiselle kyberturvallisuuden sertifiointijärjestelmälle asetettavat turvallisuustavoitteet.

Ehdotuksen mukaan sertifiointikehyksessä olisi varmistettava muun muassa, että tietoturvapalvelutarjoajilla on tarvittava osaaminen ja asiantuntemus sekä erittäin korkeatasoinen tekninen tietämys ja osaaminen kyseisellä alalla. Lisäksi tulisi varmistaa, että tietoturvapalvelut tarjotaan kaikkina aikoina erittäin laadukkaasti, palvelujen tarjoamisen yhteydessä käsiteltyjä tietoja suojellaan vahingossa tapahtuvalta muulta luvattomalta tai epätarkoituksenmukaiselta käytöltä, sekä huolehtia, että palveluita tuottavat henkilöt, ohjelmat tai koneet pääsevät ainoastaan niihin tietoihin, palveluihin tai toimintoihin, joihin heidän käyttöoikeutensa oikeuttavat.

Palveluiden toteutuksessa tulisi myös varmistaa, että tietoturvapalvelutarjoajien tuottamisessa käytettävät tieto - ja viestintätekniset tuotteet, palvelut ja prosessit ja laitteistot ovat oletusarvoisesti ja suunnitellusti turvallisia, eivät sisällä tunnettuja haavoittuvuuksia ja ovat asianmukaisesti päivitettyjä turvallisuuspäivitysten osalta.

4 Ehdotuksen oikeusperusta ja suhde suhteellisuus- ja toissijaisuusperiaatteisiin

4.1 Oikeusperusta

Kybersolidaarisuussäädösehdotuksen oikeusperustana on Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 173(3) ja 322(1)(a) artikla. Ehdotusta käsitellään noudattaen tavallista lainsäätämisjärjestystä, jossa Euroopan parlamentti ja neuvosto hyväksyvät yhdessä asetuksen. Neuvostossa edellytetään määräenemmistöpäätöksentekoa. Komission ehdotus kyberturvallisuusasetuksen muuttamisesta perustuu Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 114 artiklaan.

SEUT 173 artiklaan perustuvan toiminnan päämääränä tulee olla sen varmistaminen, että unionin teollisuuden kilpailukyvyn tarvitsemat edellytykset ovat olemassa. Artiklan mukaan tällä toiminnalla on pyrittävä erityisesti nopeuttamaan teollisuuden mukauttamista rakenteellisiin muutoksiin, edistämään kaikkialla unionissa yritysten, erityisesti pienten ja keskisuurten yritysten, aloittamisen ja kehittämisen kannalta suotuisaa toimintaympäristöä, edistämään yritysten

välisen yhteistyön kannalta suotuisaa toimintaympäristöä sekä edistämään keksintöjä, tutkimusta ja teknologista kehittämistä koskevan politiikan antamien teollisten mahdollisuuksien parempaa hyväksikäyttöä.

SEUT 173 artiklan 3 kohta mahdollistaa erityistoimenpiteet, joiden tarkoituksena on tukea jäsenvaltioissa näiden tavoitteiden toteuttamiseksi toteutettuja toimia, mutta jotka eivät käsitä jäsenvaltioiden lakien ja asetusten yhdenmukaistamista.

Asetusehdotuksen 2(2) artiklan perusteella asetusehdotuksella on kolme tavoitetta:

- Parannetaan unionin yhteistä kyberturvallisuusuhkien ja -poikkeamien havaitsemista ja niihin liittyvää tilannetietoisuutta ja vahvistetaan tätä kautta unionin teollisuuden ja palvelualojen kilpailuasemaa koko digitaalitaloudessa sekä edistetään unionin teknologista itsemääräämisoikeutta kyberturvallisuuden osalta.

- Vahvistetaan kriittisten ja erittäin kriittisten toimialojen toimijoiden varautumista kaikkialla unionissa ja solidaarisuutta kehittämällä yhteisiä toimintavalmiuksia merkittävien tai laajamittaisten kyberturvallisuuspoikkeamien varalta muun muassa tarjoamalla Digitaalinen Eurooppa -ohjelmaan osallistuville kolmansille maille unionin tukea kyberturvallisuuspoikkeamiin reagoimista varten.

- Parannetaan unionin häiriönsietokykyä ja tuetaan tehokasta reagointia tarkastelemalla ja arvioimalla merkittäviä tai laajamittaisia poikkeamia, hyödyntämällä saatuja kokemuksia ja antamalla tarvittaessa suosituksia.

Valtioneuvosto toteaa, että SEUT 173(3) artiklan oikeusperusta liittyy vahvasti yritysten toimintaedellytysten edistämiseen. Unionin tuomioistuin on muistuttanut, että artikla kuuluu unionin sisäisiä politiikkoja ja toimia koskevaan SEUT:n kolmanteen osaan, jossa se on XVII osastossa teollisuus-otsikon alla (asia C-733/19, Royaume des Pays-Bas c. Conseil de l'Union européenne et Parlament européen, 73 kohta). Valtioneuvosto toteaa, että etenkin kyberturvallisuuden eurooppalainen suojakilpi (koostuu kaikista kansallisista turvaoperaatiokeskuksista ja rajojen yli toimivista turvaoperaatiokeskuksista) sekä kyberturvallisuuspoikkeamien jälkitarkastelumekanismi (Euroopan kyberturvallisuusvirasto ENISAn tekemänä) eivät vaikuta suoraan liittyvän yritysten toimintaedellytyksiin. Unionin tuomioistuin on kuitenkin tulkinnut aiempaa EY:n perustamissopimuksen 130 artiklaa siten, että se on mahdollinen oikeusperusta, kun toteutetaan perustamissopimuksen 130 artiklan 1 kohdassa [nykyinen 173(1) artikla] esitettyjä tavoitteita, vaikka toimintalinja koskee julkista sektoria (asia C-42/97, Euroopan parlamentti v. neuvosto, kohta 60). Valtioneuvosto pitää epäselvänä, miten edellä mainitut kokonaisuudet lopulta palvelevat artiklan tavoitteita, sillä pääasiassa toimista hyötyvät jäsenvaltiot tai unionin toimielimet ja vaikutus kyberturvallisuusalaan on välillinen (vrt. asia C-42/97, Euroopan parlamentti v. neuvosto 40 ja 44 kohta). Valtioneuvosto myös katsoo, että kansallisia turvaoperaatiokeskuksia koskevalla sääntelyllä saatetaan tosiasiallisesti lähentää jäsenvaltioiden lainsäädäntöä, mikä ei ole oikeusperustan nojalla mahdollista. Sen sijaan ehdotettu kyberhätätilanteiden mekanismilla vaikutettaisiin parantavan yritystoiminnan edellytyksiä muuttuneessa kyberturvallisuusympäristössä. Kyberturvallisuusreservin muodostamisessa on kuitenkin otettava huomioon, ettei toimi voi oikeusperustan mukaan johtaa kilpailun vääristymiseen.

Kybersolidaarisuusasetusehdotus perustuu myös SEUT 322 artiklan 1 kohdan a alakohtaan. Uuden sääntelyn lisäksi ehdotuksella muutettaisiin asetusta (EU) 2021/694 (Digitaalinen Eurooppa -ohjelma). Digitaalinen Eurooppa -ohjelman oikeusperustana on SEUT 172 ja 173(3) artikla. Komission perustelumuistion mukaan kybersolidaarisuusasetuksen tulisi kuitenkin perustua myös SEUT 322(1) artiklaan, koska Digitaalinen Eurooppa -ohjelmaan esitetyillä muutoksilla

poikettaisiin maksusitoumus- ja maksumäärärahojen osalta asetuksessa (EU, Euratom) 2018/1046 (varainhoitoasetus) säädetystä vuotuisuusperiaatteesta. Varainhoitoasetuksen yhtenä oikeusperustana on SEUT 322(1) artikla. SEUT 322 artiklan 1 kohdan a alakohdan mukaan Euroopan parlamentti ja neuvosto antavat asetuksilla tavallista lainsäätämisjärjestystä noudattaen ja tilintarkastustuomioistuinta kuultuaan varainhoitosäännöt, joissa vahvistetaan varsinkin talousarvion laatimista ja toteuttamista sekä tilinpäätöksen esittämistä ja tilintarkastusta koskevat yksityiskohtaiset säännöt.

EU-tuomioistuin on vakiintuneesti katsonut, että unionin lainsäätäjän olisi mahdollisuuksien mukaan pyrittävä aina käyttämään vain yhtä oikeusperustaa. Kahden tai useamman rinnakkaisen oikeusperustan käyttäminen on poikkeuksellinen ratkaisu. Se on EU-tuomioistuimen mukaan mahdollista silloin, kun on kyse toimesta, jolla on useampi samanaikainen tarkoitus tai sillä on useita osatekijöitä, joita ei voida erottaa toisistaan ja joista mikään ei ole toiseen nähden toisarvoinen ja välillinen. Valtioneuvoston arvion mukaan nyt on kyse tällaisesta tilanteesta. Ehdotuksella ei ole yhtä pääasiallista tarkoitusta tai määräävää tekijää, vaan se koostuu kahdesta keskenään eroavasta osatekijästä, josta rahoitusta koskeva osuus on erotettavissa muusta sisällöstä. Lisäksi useamman oikeusperustan käyttäminen edellyttää aina sitä, että ne ovat keskenään yhteensopivia. Myös tämä edellytys täyttyy, sillä päätöksentekomenettely on molemmissa oikeusperustoissa sama.

Näin ollen valtioneuvosto katsoo ehdotetusta kybersolidaarisuusasetuksesta, että

- SEUT 173(3) artikla ei vaikuta asianmukaiselta oikeusperustalta kyberturvallisuuden eurooppalaiselle suojakilvelle eikä kyberturvallisuuspoikkeamien jälkitarkastelumekanismille, ellei sääntelyn yhteyttä teollisuuteen ja lainsäädännön lähentämiseen selkeytetä

- SEUT 173(3) artikla vaikuttaa asianmukaiselta oikeusperustalta kyberhätätilanteiden mekanismille

- SEUT 322 oikeusperusta vaikuttaa asianmukaiselta oikeusperustalta vuotuisuusperiaatteesta poikkeamiseen

- kahden oikeusperustan käyttäminen vaikuttaa perustellulta.

Kyberturvallisuusasetukseen ehdotettavan muutoksen oikeusperustana on SEUT 114 artikla. Sen mukaan sisämarkkinoiden toteuttamiseksi parlamentti ja neuvosto toteuttavat toimenpiteet jäsenvaltioiden lakien, asetusten ja hallinnollisten määräysten lähentämiseksi.

SEUT 114 artiklan mukaan neuvosto hyväksyy ehdotuksen määräenemmistöllä yhdessä Euroopan parlamentin kanssa tavallisessa lainsäätämisjärjestyksessä. EU-tuomioistuin on vakiintuneesti katsonut, että säädös voidaan hyväksyä SEUT 114 artiklan perusteella ainoastaan, mikäli siitä ilmenee ”objektiivisesti ja tosiasiallisesti, että sen tarkoituksena on sisämarkkinoiden toteuttamista ja toimintaa koskevien edellytysten parantaminen”. Mikäli tämä edellytys täyttyy, antaa SEUT 114 artikla unionin lainsäätäjälle laajan harkintavallan kulloinkin tarvittavien lähentämis- ja yhdenmukaistamistoimenpiteiden valinnassa.

Komissio katsoo, että kuten muutettavan kyberturvallisuusasetuksen tapauksessa, ehdotuksella pyritään välttämään sisämarkkinoiden pirstoutumista erityisesti mahdollistamalla eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttöön ottaminen tietoturvapalveluille. Jä-

senvaltiot ovat jo alkaneet ottaa käyttöön kansallisia tietoturvapalvelujen sertifiointijärjestelmiä. Näin ollen on olemassa konkreettinen riski tällaisten palvelujen sisämarkkinoiden pirstoutumisesta, mitä tällä ehdotuksella pyritään estämään.

Valtioneuvosto toteaa, että esitetty oikeusperusta on sama kuin alkuperäisellä kyberturvallisuusasetuksella. Valtioneuvosto voi yhtyä komission esittämiin perusteluihin sisämarkkinoiden toteuttamisen ja toiminnan parantamisesta ehdotuksella. Näin ollen valtioneuvosto katsoo, että SEUT 114 artikla vaikuttaa asianmukaiselta oikeusperusta kyberturvallisuusasetukseen ehdotetulle muutokselle.

4.2 Toissijaisuus- ja suhteellisuusperiaate

Euroopan unionista tehdyn sopimuksen toissijaisuus- ja suhteellisuusperiaatteita koskevan 5 artiklan mukaisesti unioni voi antaa säädöksiä ainoastaan silloin, kun se on tarpeen ja ainoastaan siinä laajuudessa, kun se on tarpeen. SEU 5 artiklan 3 kohdassa määrätyn toissijaisuusperiaatteen mukaisesti unioni toimii aloilla, jotka eivät kuulu sen yksinomaiseen toimivaltaan, ainoastaan jos ja siltä osin kuin jäsenvaltiot eivät voi riittävällä tavalla saavuttaa suunnitellun toiminnan tavoitteita, vaan ne voidaan suunnitellun toiminnan laajuuden tai vaikutusten vuoksi saavuttaa paremmin unionin tasolla.

Komissio katsoo kybersolidaarisuusasetusehdotuksen olevan Euroopan unionista tehdyn sopimuksen (SEU) 5 artiklassa tarkoitetun toissijaisuusperiaatteen mukainen. Komission mukaan ehdotuksen tavoitteet eivät ole tehokkaasti toteutettavissa jäsenvaltioiden kansallisen lainsäädännön tasolla kyberturvallisuusuhkien rajat ylittävän luonteen vuoksi. Komissio katsoo, että eri mekanismien kautta annettava tuki täydentää kansallisia kyvykkyyksiä olematta päällekkäinen olemassa olevien kyberuhkien havainnointi, varautumis-, ja vastaamistoimien kanssa.

Komissio katsoo, että kybersolidaarisuusasetusehdotuksessa esitettävät toimet eivät vaikuta jäsenvaltioiden vastuuseen kansallisesta turvallisuudesta, yleisestä turvallisuudesta, rikosten ehkäisemisestä, tutkimisesta, paljastamisesta ja syytteeseenpanosta. Komissio katsoo myös, että toimet eivät myöskään vaikuta NIS2-direktiivin soveltamisalaan kuuluvien toimijoiden oikeudellisiin velvoitteisiin yhteisöjen oikeudellisiin velvoitteisiin toteuttaa kyberturvallisuustoimenpiteitä NIS2-direktiivin mukaisesti vaan täydentävät tällaisia toimia ja toimenpiteitä tukemalla parantamalla uhkien havainnointia.

Valtioneuvosto katsoo, että ehdotus on pääosin toissijaisuusperiaatteen mukainen, vaikka arviointia vaikeuttaa vaikutusarvioinnin puuttuminen. On selvää, että jäsenvaltioiden yhteistyötä ja tiedonvaihtoa on tarpeen edistää EU:n tasolla ja näin on tehty myös aiemmin esimerkiksi NIS2-direktivin mukaisessa yhteistyöryhmässä, CSIRT-verkostossa ja EU-CyCLONe-verkostossa sekä Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskuksen kautta (asetus (EU) 2021/887). Suomella on toisaalta jo nyt verrattain kehittyneet menetelmät ja pitkällä aikavälillä muodostuneet yhteistoiminta- ja luottamusverkostot, joita edelleen kehitetään NIS2-direktiivissä määritellyn CSIRT- ja CyCLONe-verkostojen myötä. Voidaan kuitenkin arvioida, että ehdotetusta SOC-verkostosta on mahdollisesti saatavissa myös Suomen kannalta jonkin verran hyötyä, vaikka Suomi ei välttämättä ole merkittävin hyötyjä ehdotuksesta.

Valtioneuvosto kuitenkin huomauttaa, että SEU 4(2) artiklan nojalla kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla. Ehdotetun 1(3) artiklan mukaan asetus ei vaikuta jäsenvaltioiden *ensisijaiseen* vastuuseen kansallisesta turvallisuudesta. Valtioneuvosto katsoo, että ottaen huomioon kybersolidaarisuusasetusehdotuksen toimenpiteiden kohdentumisen,

jotka monilla tavoin ovat liitoksissa kansallisen turvallisuuden kysymyksiin, on jatkovalmistelussa arvioitava erityisesti ehdotuksen suhdetta kansalliseen turvallisuuteen, joka kuuluu yksinomaan kunkin jäsenvaltion vastuulle.

Toiseksi valtioneuvosto huomauttaa, että – oikeusperustaan liittyvien rajoitusten lisäksi – toissijaisuusperiaatteen mukaista ei ole rajoittaa jäsenvaltioiden hallinnollista autonomiaa määrittämällä, että kansallisen turvaoperaatiokeskuksen on oltava nimenomaan julkisoikeudellinen laitos (2(1)(2) ja 4(1) artikla).

Komissio katsoo kyberturvallisuusasetukseen ehdotetun muutoksen olevan toissijaisuusperiaatteen mukainen, koska eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien käyttöön ottaminen tietoturvapalveluille voidaan saavuttaa ainoastaan unionin tason toimilla ja tällä vältetään sisämarkkinoiden pirstoutuminen. Lisäksi komission mukaan ehdotetun muutoksen kohteena olevien tietoturvapalvelujen tarjoajat sekä niiden suurimmat potentiaaliset asiakkaat toimivat koko unionin laajuisesti. Valtioneuvosto voi yhtyä komission esittämiin perusteluihin ehdotuksen toissijaisuusperiaatteen mukaisuudesta.

SEU 5 artiklan 4 kohdassa määrätyn suhteellisuusperiaatteen mukaisesti unionin toiminnan sisältö ja muoto eivät saa ylittää sitä, mikä on tarpeen perussopimusten tavoitteiden saavuttamiseksi. Näin ollen lainsäätäjän on suhteellisuusperiaatteen noudattamiseksi valittava silloin, kun vaihtoehtoja on useampia, vaikutuksiltaan lievin vaihtoehto, jolla tavoite voidaan tehokkaasti saavuttaa. Komission arvion mukaan ehdotetut toimenpiteet kybersolidaarisuusasetuksen osalta eivät mene pidemmälle kuin mitä on tarpeen ehdotuksen tavoitteiden saavuttamiseksi. Se ei vaikuta jäsenvaltioiden velvollisuuksiin kansalliseen turvallisuuteen liittyen, eikä se vaikuta NIS2-direktiivin mukaisten toimijoiden velvoitteisiin. Ehdotetut toimenpiteet täydentävät ja tukevat uhkien havaitsemiseen ja analysointiin liittyvän infrastruktuurin luomista.

Valtioneuvosto katsoo, että ehdotus ei kaikilta osin olisi suhteellisuusperiaatteen mukainen. Yleisesti on huomioitava, ettei rahoitusinstrumenttien kautta luoda eri jäsenvaltioille vääränlaisia kannustimia, jotka eivät motivoisi jäsenmaita omien kyberturvallisuuskyvykkyyksien kehittämiseen.

Valtioneuvosto arvioi, että etenkin ehdotettu eurooppalaista kybersuojakilpeä koskeva sääntely ei täytä suhteellisuusperiaatteen vaatimuksia. Ehdotuksessa ei ole riittävästi huomioitu olemassa olevia yhteistyörakenteita ja ehdotuksella luodaan uutta hallinnollista rakennetta näiden päälle. Erityisen olennaista olisi huomioida EU:n verkko- ja tietoturvadirektiivin 2016/1148 mukainen CSIRT-verkosto, jolla on jo olemassa tehtäviä kyberuhkien, haavoittuvuuksien ja poikkeamien seurantaan liittyen. Lisäksi CSIRT-verkoston tehtäviä tarkennetaan ja laajennetaan uudessa NIS2-direktiivissä. Huomionarvoista on myös se, että ehdotetut SOC-toimijat olisivat hyvin suurella todennäköisyydellä samoja, kuin kansalliset CSIRT-yksiköt.

SOC-verkostoon liittyvän tiedonvaihdon osalta on tunnistettu riski siitä, että ehdotus kääntyy tosiasiassa tavoitteitaan vastaan. Kyberturvallisuuteen liittyvä tiedonvaihto on perinteisesti perustunut toimijoiden väliseen luottamukseen. Ehdotus ei täsmennä riittävästi sitä, minkälaisesta ja tasoisesta tiedonvaihdosta ehdotuksessa tosiasiassa on kyse, miten ja mikä tieto liikkuu eri SOC-verkostojen välillä ja miten sitä on mahdollista luovuttaa esimerkiksi yksityiselle sektorille, jolloin on mahdollista, että tiedonvaihtoa tämän seurauksena vähennetään lisäämisen sijaan. Tosiseikkojen riittävä arviointi on kuitenkin haastavaa vaikutusarvioinnin puuttumisen vuoksi ja asiaan onkin kiinnitettävä erityistä huomiota neuvottelujen aikana.

Kyberturvallisuusasetuksen osalta komissio arvioi, että ehdotettu aloite on oikeassa suhteessa tavoitteeseen nähden, sillä ehdotetuilla muutoksilla kyberturvallisuusasetukseen mukautetaan

kyberturvallisuuden sertifiointikehyksen soveltamisalaa siten, että siihen sisällytetään ”tietoturvapalvelut”, määritellään kyseiset palvelut NIS 2 -direktiivin mukaisesti ja muutetaan eurooppalaisen kyberturvallisuuden sertifioinnin turvallisuustavoitteita ”tietoturvapalveluien” huomioon ottamiseksi. Valtioneuvosto voi yhtyä komission esittämiin perusteluihin ehdotuksen suhteellisuusperiaatteen mukaisuudesta.

4.3 Toimivallan siirto sekä komissiolle ehdotetut tehtävät

Ehdotettuun kybersolidaarisuusasetukseen sisältyy täytäntöönpanovallan siirtämistä komissiolle. Komissiolla on valtuudet antaa 21 artiklassa tarkoitetun tarkastelumenettelyn mukaisesti täytäntöönpanosäädöksiä, joilla

- määritetään edellytykset, jotka koskevat rajojen yli toimivien turvaoperaatiokeskusten välistä yhteentoimivuutta (6(3) artikla)
- vahvistetaan menettelylliset järjestelyt, jotka koskevat mahdollisiin tai käynnissä oleviin laajamittaisiin kyberturvallisuuspoikkeamiin liittyvien tietojen jakamista rajojen yli toimivien turvaoperaatiokeskusten ja unionin elinten välillä (7(2) artikla)
- säädetään tekniset vaatimukset, joiden avulla varmistetaan tietosuojan ja infrastruktuurin korkea fyysisen turvallisuuden taso ja suojellaan unionin turvallisuuteen liittyviä etuja jaettaessa tietoja muiden toimijoiden kuin jäsenvaltioiden julkisten elinten kanssa (8(3) artikla)
- määritetään EU:n kyberturvallisuusreserviä varten tarvittavien poikkeamienhallintapalvelujen tyyppi ja määrä (12(8) artikla)
- määritetään tarkemmin yksityiskohtaiset järjestelyt, jotka koskevat EU:n kyberturvallisuusreservin tukipalvelujen kohdentamista (13(7) artikla).

Valtioneuvosto pitää ehdotettua toimivallan siirtoa pääosin asianmukaisena. Tietojenvaihdon käytännön toteuttamiseen liittyy teknisiä kysymyksiä, joita on syytä yhdenmukaistaa. Täytäntöönpanovaltuuksia olisi kuitenkin vielä syytä selventää niin, että siinä viitattaisiin selvemmin tekniseen yhteentoimivuuteen erotuksena toiminnallisen tai hallinnollisen yhdenmukaisuudesta syntyvästä yhteentoimivuudesta. Jäsenvaltioiden hallinnollinen autonomia on yksi unionioikeuden lähtökohdista eikä asetuksen oikeusperusta mahdollista jäsenvaltioiden lainsäädännön lähentämistä. Myöskään vaihdettavia tietoja ei voi jättää alemman aseteisen sääntelyn varaan, jos kyse on muista kuin julkisista tiedoista, sillä valtioneuvoston käsityksen mukaan kyse olisi silloin sääntelyn olennaisesta sisällöstä (ks. myös jäljempänä perustuslakia koskeva jakso). Valtioneuvosto myös katsoo, että poikkeamienhallintapalveluiden tyypit olisi asianmukaista ainakin jollain tasolla nostaa ehdotettuun asetukseen, koska kyse voisi olla sääntelyn olennaisesta sisällöstä. Tarjottavat palvelut voivat nimittäin välillisesti vaikuttaa siihen, millaisia omia kyvykkyyksiä ja toimenpiteitä jäsenvaltiot haluavat itse rahoittaa.

Komissiolle ositettaisiin myös eräitä tehtäviä. Komissio nimeäisi ne toimialat tai toimialan osat, joiden toimijoihin voidaan soveltaa koordinoitua varautumisen testausta (11(1) artikla). Komissio myös määrittäisi EU:n kyberturvallisuusreservin painopisteet ja kehityksen sekä valvoo sen täytäntöönpanoa (12(5) artikla). Asetusehdotuksessa ei kuitenkaan määritellä, miten tämä tapahtuisi. Komissio arvioisi EU:n kyberturvallisuusreservistä haettavaa tukea koskevat pyynnöt (14(1) artikla). Valtioneuvosto katsoo, että kyberturvallisuusreservistä haettavien tukien pyyntöjen käsittelyn vastuu soveltuisi paremmin komission sijaan Euroopan kyberturvallisuusvirasto

ENISAlle. Valtioneuvosto katsoo, että jäsenvaltiot olisi hyvä ottaa mukaan varautumistestausten kohdentamisen sekä kyberturvallisuusreservin painopisteiden arviointiin.

5 Ehdotuksen vaikutukset

Komissio ei ole tehnyt vaikutustenarviointia kybersolidaarisuussäädösehdotuksesta. Komissio perustelee vaikutusarvioinnin puuttumista säädösehdotuksen kiireellisyydellä. Komission mukaan ehdotus ei aiheuta merkittäviä hallinnollisia tai ympäristövaikutuksia, jotka muuttaisivat Digitaalinen Eurooppa-ohjelmaan tehdyn vaikutustenarvioinnin arviota. Varautumistestausten ja häiriövastepalveluiden (kyberhätätilanteiden mekanismi) osalta komissio on huomioinut ehdotuksessa vuonna 2022 käynnistetyn ENISAn pilottiprojektin toteutuksesta saatuja oppeja.

Ehdotuksen kansallisia vaikutuksia on vaikea arvioida komission vaikutusarvioinnin puuttuessa. Suomeen ja suomalaisiin toimijoihin kohdistuvia vaikutuksia arvioidaan tarkemmin käsittelyn edetessä.

5.1 Taloudelliset vaikutukset

Ehdotuksella on vaikutuksia suoraan valtiontalouteen, yrityksiin ja välillisesti yrityksille ja kotitalouksille. Komission arvion mukaan ehdotuksella lisätään 100 miljoonaa euroa kyberturvallisuuden erityistavoitteelle DEP-ohjelmaan uudelleenjärjestelemällä ohjelman määrärahoja toisista erityistavoitteista. Muutokset DEP-ohjelman rahoituksessa voivat heikentää muiden ohjelman tavoitteiden saavuttamista (mm. tekoäly ja digitaalinen osaaminen). Ehdotuksen rahoitusmekanismeista tarvitaan lisää tietoja ennen kuin ehdotuksen kansallisten taloudellisten vaikutusten arviointia voidaan tehdä riittävällä tasolla. Ehdotukseen sisältyvän kybersuojakilven hankintoihin sisältyy kansallinen rahoitusosuus, joka on 25-50 % kokonaiskustannuksista.

Ehdotuksella tulee olemaan valtiontaloudellisia vaikutuksia lisääntyvien viranomaistehtävien myötä. Vaikutukset tarkentuvat kansallisen toimeenpanon vaiheen vaikutusarvioinneissa.

Ehdotus edellyttää kansallisen turvaoperaatiokeskuksen nimeämistä. Tämä voi edellyttää lainsäädäntömuutoksia sekä muutoksia kansallisten viranomaisten tehtäviin ja viranomaisten toimintaan liittyvien määrärahojen uudelleenarviointia lisäresurssitarpeista johtuen.

Rajojen yli toimivaan turvaoperaatiokeskusten yhteenliittymään liittyminen vaikuttaisi kansallisesti tällä hetkellä tehtäviin kybertilannekuvapalveluiden hankintoihin ja voisi mahdollisesti tuoda hankintoihin liittyviä säästöjä pidemmällä aikavälillä.

Kyberturvallisuusreservi voi luoda unionin alueella luotettaville palveluntarjoajien kriteerit täyttäville kyberturvallisuusalan yrityksille uusia liiketoimintamahdollisuuksia häiriövastepalveluiden toteutuksessa. Vaatimus palveluiden tuottamisesta kohdemaan kielellä voi toisaalta vähentää Suomeen saatavilla olevien palveluntarjoajien määrää ja toisaalta heikentää suomalaisten tietoturva-alan yritysten liiketoimintamahdollisuuksia muissa jäsenmaissa. Suomalaisilla tiettyjen toimialojen yrityksillä olisi mahdollista myös saada edellytysten täyttyessä apua kyberturvallisuusreservistä, mitä voidaan pitää yritysten toiminnan kannalta positiivisena.

Suomi pyytää työryhmäkäsittelyn kuluessa lisäselvitystä komissiolta vaikutuksista.

5.2 Vaikutukset viranomaistoimintaan

Rajojen yli toimivan SOC-yhteenliittymän toiminta olisi osittain päällekkäistä nykyisten tiedonvaihto- ja tilannekuvamekanismien kanssa. Toimiva tiedonvaihto rajojen yli toimivassa

SOC-yhteenliittymässä voisi parantaa Suomessa tiettyjen viranomaisten kybertilannekuvatiedon keräämistä. Verkostojen toiminta perustuu kuitenkin osallistuvien maiden aktiivisuuteen. Kansainvälisten verkostojen määrän kasvaessa tulee kyetä priorisoimaan tärkeimmät verkostot suhteessa käytössä oleviin resursseihin.

Ehdotus edellyttää myös kansallisen kyberkriisinhallintaviranomaisen tai CSIRT-toimijan toimimista yhteyspisteenä kyberturvallisuusreservin palveluiden hakemisessa. Suomessa keskitettynä yhteyspisteenä toimisi Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus.

Kyberhätätilanteiden mekanismin mukaiset varautumistestaukset kriittisille toimialoille voi parantaa Suomen ja EU:n tasolla kyberturvallisuutta, kun yritysten kybersuojauksista voidaan tunnistaa puutteita ennakollisesti.

5.3 Kyberturvallisuusasetukseen ehdotettujen muutosten vaikutukset

Kyberturvallisuusasetukseen ehdotettujen muutosten osalta komissio ei ole toteuttanut vaikutustenarviointia perustuen ehdotuksen suppeuteen.

Kyberturvallisuusasetukseen ehdotetut muutokset tietoturvapalveluiden sertifiointikehyksestä voisivat yhdenmukaistaa unionin alueella toimivien tietoturva-alan yritysten toiminnalle asetettuja laatu- ja turvallisuusvaatimuksia. Tämä voisi parantaa eurooppalaisten tietoturva-alan yritysten kilpailukykyä suhteessa unionin ulkopuolisiin yrityksiin ja parantaa niiden palveluiden laatua ja luotettavuutta. Sertifiointikehys voisi kuitenkin lisätä pienten ja keskisuurten alan yritysten hallinnollista ja taloudellista taakkaa ja heikentää niiden liiketoimintamahdollisuuksia.

Kyberturvallisuusasetukseen ehdotetuilla muutoksilla ei olisi vaikutuksia kansalliseen lainsäädäntöön tai suoraan vaikutuksia valtiontalouteen.

6 Ehdotuksen suhde perustuslakiin sekä perus- ja ihmisoikeuksiin

Komission mukaan ehdotus parantaa digitaalisten tietojen turvallisuutta ja auttaa siten suojelemaan oikeutta vapauteen ja turvallisuuteen EU:n perusoikeuskirjan 6 artiklan mukaisesti ja oikeutta yksityis- ja perhe-elämän kunnioittamiseen EU:n perusoikeuskirjan 7 artiklan mukaisesti. Lisäksi komission mukaan ehdotus suojelee yrityksiä taloudellisesti vahingollisilta kyberhyökkäyksiltä ja edistää siten elinkeinovapautta EU:n perusoikeuskirjan 16 artiklan mukaisesti ja omistusoikeutta EU:n perusoikeuskirjan 17 artiklan mukaisesti. Lisäksi komission mukaan ehdotuksella suojellaan kriittistä infrastruktuuria kyberhyökkäyksiltä ja edistetään siten oikeutta terveydenhuoltoon EU:n perusoikeuskirjan 35 artiklan mukaisesti ja oikeutta mahdollisuuteen käyttää yleistä taloudellista etua koskevia palveluja EU:n perusoikeuskirjan 36 artiklan mukaisesti.

Valtioneuvosto voi yhtyä komission näkemyksiin, joskin komission mainitsemat vaikutukset ovat valtioneuvoston näkemyksen mukaan pääasiassa välillisiä. Ehdotus voi välillisesti myös edistää myös perusoikeuskirjan 8 artiklan ja perustuslain 10 §:ssä turvattua henkilötietojen suojaa ehkäisemällä tietoturvaloukkauksia. Valtioneuvoston näkemyksen mukaan ehdotuksesta hyötyvät pääasiassa julkisen sektorin elimet. Tietoturvaloukkausten ehkäisemisellä on siten yhteys perustuslain 12 §:n 2 momentissa säädetyn asiakirjajulkisuuden ja salassapidon sekä perustuslain 21 §:ssä säädettyjen hyvän hallinnon oikeusturvan vaatimusten toteuttamisessa tiedonhallinnassa.

Tästä huolimatta valtioneuvosto toteaa, että osaa ehdotetun kybersolidaarisuusasetuksen sääntelystä on tarkasteltava lähemmin perustuslakia ja perustuslakivaliokunnan käytäntöä vasten.

Lakiperusteisuus sekä julkisen hallintotehtävän siirtäminen (PL 2 ja 124 §)

Ehdotettu kyberturvallisuuden eurooppalainen suojakilpi rakentuu kansallisten turvaoperaatiokeskusten päälle (3(1) artikla). Jokaisen jäsenvaltion on nimettävä niitä vähintään yksi. Kansallisen turvaoperaatiokeskuksen tulee olla julkisoikeudellinen laitos. Se toimisi ”julkisten ja yksityisten organisaatioiden viitetahona ja yhdyskäytävänä kyberturvallisuusuhkia ja -poikkeamia koskevien tietojen keräämistä ja analysointia sekä rajojen yli toimivan turvaoperaatiokeskuksen toiminnan edistämistä varten” ja sillä ”olisi oltava käytössään uusimman tason teknologiaa, jolla kyberturvallisuusuhkiin ja -poikkeamiin liittyviä tietoja voidaan havaita, yhdistää ja analysoida”. (2(1)(2) ja 4(1) artikla.)

Perustuslain 124 §:n mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle. Valtioneuvosto toteaa, että kyberturvallisuuspuolella toimii viranomaisten lisäksi yksityisiä toimijoita, jotka keräävät ja analysoivat tietoa kyberuhista ja -tapahtumista. Valtioneuvosto kuitenkin katsoo, että kansallisen turvaoperaatiokeskuksen toimiminen eräänlaisena solmukohtana voisi tehdä tehtävästä julkisen hallintotehtävän (vrt. liikenne- ja viestintävirastosta annetun lain 3 §, jossa kyberturvallisuuskeskuksen yhtenä tehtävänä on ylläpitää kansallista kyberturvallisuuden tilannekuvaa ja tukea toimialallaan yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin). Komission ehdotuksen perusteella ei voida myöskään täysin poissulkea sitä, ettei tehtävään sisältyisi merkittävää julkisen vallan käyttöä. Nimittäin kansallisista turvaoperaatiokeskuksista koostuviin rajojen yli toimiviin turvaoperaatiokeskuksiin ja kyberturvallisuuden eurooppalaiseen suojakilpeen sisältyisi laajaa tietojenvaihtoa (3(2), 6 ja 7(1) artikla) eikä esimerkiksi julkisuuslain 24 §:n 1 momentin 3, 7, 9 ja 20 kohdan mukaista salassa pidettävää tietoa, henkilötietoa tai sähköisen viestinnän palveluista annetussa laissa tarkoitettuja sähköisen viestinnän välitystietoja ole rajattu tietojenvaihdon ulkopuolelle (henkilötiedoista ks. johdanto-osan 22 perustelukappale ja luottamuksellisista tiedoista 23 perustelukappale). Lisäksi valtioneuvosto kiinnittää huomiota siihen, että rajojen yli toimivan turvaoperaatiokeskuksen yhtenä tavoitteena on ”tukea korkealaatuisen tiedustelutiedon tuottamista” (2(1)(1) artikla). Näin ollen valtioneuvoston katsoo, että ehdotus ei ole ongelmaton perustuslain 124 §:n kannalta, vaan ehdotusta on tästä näkökulmasta täsmennettävä.

Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin. Kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia.

Valtioneuvosto toteaa, että kybertuvallisuuden eurooppalaisen suojakilven toiminta vaikuttaisi perustuvan pitkälti sopimuksiin yhtäältä jäsenvaltioiden kesken sekä jäsenvaltioiden yhteenliittymien ja unionin elinten kesken. Tältä osin valtioneuvosto kiinnittää huomiota siihen, että rajojen yli toimivaa turvaoperaatiokeskusta luonnehditaan ”usean maan kattavaksi foorumiksi” sekä ”koordinoiduksi verkostorakenteeksi” (2(1)(1) artikla). Rajojen yli toimiva turvaoperaatiokeskus perustuisi sopimukseen (isännöintiyhteenliittymä), jonka kansalliset turvaoperaatiokeskukset ovat tehneet (2(1)(3), 5(3) ja 6(3) artikla). Rajojen yli toimivalla turvaoperaatiokeskuksella tulisi olla laillinen edustaja ja se voisi ilmeisesti myös olla oikeushenkilö (5(4) artikla) ja tehdä yhteistyösopimuksia muiden rajojen yli toimivien turvaoperaatiokeskusten kanssa (6(4) artikla) sekä isännöinti- ja käyttösopimuksen Euroopan kyberturvallisuuden osaamiskeskuksen kanssa hankittavista välineistä ja infrastruktuurista (5(2) artikla). Rajojen yli toimivat turvaoperaatiokeskukset ja kansalliset turvaoperaatiokeskukset puolestaan muodostaisivat suoraan asetuksen nojalla kyberturvallisuuden eurooppalaisen suojakilven (3(1) artikla).

Valtioneuvosto pitää rakennetta verrattain monimutkaisena. Jos kyseessä olisi edellä kuvatusti viranomaistehtävä, valtioneuvosto katsoo, että rakenne ei ole ongelmitta yhteensovitettavissa viranomaistoiminnan lakiperusteisuuden kanssa. Perustuslakivaliokunta on katsonut, että viranomaisten yhteistoimintasopimusta on arvioitava perustuslain 2 §:n 3 momentin kannalta. Perustuslakivaliokunta ei esimerkiksi ole pitänyt valtiosääntöoikeudellisesti asianmukaisena, että viranomaisen yksityisiin kohdistuvaa julkista valtaa sisältävä toimivalta voisi rajoitetulta osiltakaan pohjautua viranomaisten väliseen sopimukseen. (PeVL 19/2005, s. 8/I.) Niin ikään viranomaisten välinen mahdollisten salassa pidettävien tietojen vaihto ei voi perustua sopimukseen, mitä käsitellään tarkemmin jäljempänä.

Kansallinen turvaoperaatiokeskus voi tehdä Euroopan kyberturvallisuuden osaamiskeskuksen kanssa yhteishankintasopimuksen. Tämä edellyttää isännöinti- ja käyttösopimuksen tekemistä hankittavista välineistä ja infrastruktuurista. (4 artiklan 2 kohta.) Valtioneuvosto toteaa selvyyden vuoksi, että hankintaan liittyvä hallintosopimus ei itsessään ole perustuslain kannalta ongelmallinen, kunhan edellä mainitut perustuslain 2 §:n 3 momentista juontuvat vaatimukset otetaan huomioon.

Myös ehdotetun EU:n kyberturvallisuusreservin käyttöä on syytä vielä tarkastella perustuslain 124 §:ää vasten. Reservin käyttäminen vaikuttaa pakolliselta silloin, kun viranomaiset reagoivat itseensä kohdistuviin merkittäviin tai laajamittaisiin poikkeamiin tai tukevat kriittisten alojen toimijoita niihin reagoimisessa (12(4) artikla).

Yksityiselämän suoja, henkilötietojen suoja, sähköisen viestinnän tietosuoja sekä julkisuusperiaate (PL 10 ja 12 §)

Perustuslain 10 §:n 1 ja 2 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Perustuslain 10 §:n 4 momentin perusteella viestin salaisuuteen voidaan kuitenkin lailla säätää tiettyjä välttämättömiä rajoituksia.

Perustuslain 12 §:n 2 momentin mukaan viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta.

Valtioneuvosto huomauttaa ensinnäkin, että viranomaisen keräämät, pyytämät tai sille toimitetut tiedot ovat viranomaisen asiakirjoja. Niiden julkisuus- ja salassapito määräytyy julkisuuslainsäädännön mukaan. Asetuksen suhde kansalliseen julkisuussääntelyyn mukaan lukien salassapito jää epäselväksi. Asetuksessa on vain yleisluonteisia viittauksia esimerkiksi luottamuksellisuuteen ja turvallisuuteen (johdanto-osan 23 perustelukappale, 8(1) ja 18(3) artikla).

Valtioneuvosto huomauttaa toiseksi, kuten edellä on jo todettu, että kyberturvallisuuden eurooppalaiseen suojakilpeen sekä rajojen yli toimivaan turvaoperaatiokeskukseen sisältyy laajaa tietojenvaihtoa eikä esimerkiksi julkisuuslain 24 §:n 1 momentin 3, 7 ja 20 kohdan mukaista salassa pidettävää tietoa, henkilötietoa tai sähköisen viestinnän palveluista annetussa laissa tarkoitettuja sähköisen viestinnän välitystietoja ole rajattu tietojenvaihdon ulkopuolelle. Kyberturvallisuuden eurooppalaisen suojakilven puitteissa tapahtuvaa tietojenvaihtoa ei ole tarkemmin määritelty (3(2)(a) artikla). Sen sijaan isännöintiyhteenliittymän jäsenet vaihtavat keskenään ”asiaankuuluvia tietoja”, ja vaihdettava tiedot ja tietojenvaihdon tarkoitus olisi määritelty asetuksessa. (6(1) artikla.) Samoin ”asiaankuuluvat tiedot” mahdollisesta tai käynnissä olevasta laajamittaisesta kyberturvallisuuspoikkeamasta tulisi toimittaa tietyille EU-elimille (7(1) artikla).

Perustuslakivaliokunta on kiinnittänyt erityistä huomiota siihen, että arkaluonteisten tietojen käsittely on rajattava täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään ja sääntelyn on oltava tietosuoja-asetuksen mahdollistamissa puitteissa yksityiskohtaista ja kattavaa (ks. esim. PeVL 4/2021 vp, 4 kohta). Perustuslakivaliokunta on arvioinut viranomaisten tietojen saamista ja luovuttamista salassapitovelvollisuuden estämättä koskevaa sääntelyä perustuslain 10 §:n 1 momentissa säädetyn yksityiselämän ja henkilötietojen suojan kannalta ja kiinnittänyt huomiota muun muassa siihen, mihin ja ketä koskeviin tietoihin tiedonsaantioikeus ulottuu ja miten tiedonsaantioikeus sidotaan tietojen välttämättömyyteen. Viranomaisen tietojensaantioikeus ja tietojenluovuttamismahdollisuus ovat voineet liittyä jonkin tarkoituksen kannalta "tarpeellisiin tietoihin", jos tarkoitetut tietosisällöt on pyritty luettelemaan laissa tyhjentävästi. Jos taas tietosisältöjä ei ole samalla tavoin luetteloitu, sääntelyyn on pitänyt sisällyttää vaatimus "tietojen välttämättömyydestä" jonkin tarkoituksen kannalta. Valiokunta on antanut erityistä merkitystä luovutettavien tietojen luonteelle arkaluonteisina tietoina arvioidessaan täsmällisyyttä ja sisältöä. Mikäli ehdotetut säännökset tietojen luovutuksesta ovat kohdistuneet myös arkaluonteisiin tietoihin, on tavallisen lain säätämisjärjestyksen käyttämisen edellytyksenä ollut sääntelyn täsmentäminen selostetun perustuslakivaliokunnan viranomaisten tietojen saamista ja luovuttamista salassapitovelvollisuuden estämättä koskevaa sääntelyä koskevan käytännön mukaiseksi. Valiokunta ei toisaalta ole pitänyt hyvin väljiä ja yksilöimättömiä tietojensaantioikeuksia perustuslain kannalta mahdollisina edes silloin, kun ne on sidottu välttämättömyyskriteeriin (ks. esim. PeVL 4/2021 vp, 10 kohta ja siinä viitatut lausunnot).

Valtioneuvosto katsoo, että asetuksen sääntelyä tulee täsmentää, jotta sen suhde julkisuusperiaatteeseen selkenee. Lisäksi tulee selkeyttää, missä määrin asetus velvoittaa tietojenvaihtoon ja sisältyisikö tietojenvaihtoon julkisuuslain mukaan salassa pidettävien tietojen vaihtoa, henkilötietojen vaihtoa taikka viestinnän sisällön tai viestinnän välitystietojen vaihtoa. Valtioneuvosto katsoo, että tietojenvaihtoon liittyvät valtiosääntöiset reunaehdot on otettava paremmin esityksessä huomioon. Valtioneuvosto pitää myös tarpeellisena täsmentää esitystä niin, että esimerkiksi vaihdettavia tietosisältöjä, suojatoimia, käyttötarkoituksia ja tietojen poistamista ei jätettäisi yhteistyösopimusten (6(4) artikla) tai komission täytäntöönpanosäädösten varaan (6(3), 7(2) ja 8(3) artikla), vaan nämä koskisivat vain teknisiä näkökulmia.

Myös ehdotetun EU:n kyberturvallisuusreservin käyttöä on syytä vielä tarkastella edellä mainittuja näkökulmia vasten. Kyberreservin käyttöön liittyy tietojen antamista (12(4) ja (5) ja 14(6) artikla).

Omaisuuden suoja ja elinkeinovapaus (PL 15 ja 18§)

Perustuslain 15 §:n mukaan jokaisen omaisuus on turvattu.

Perustuslain 18 §:n 1 momentin mukaan jokaisella on oikeus lain mukaan hankkia toimeentulonsa valitsemallaan työllä, ammatilla tai elinkeinolla.

Ehdotettuun kyberhätätilanteiden mekanismiin sisältyy kriittisten toimialojen varautumisen koordinoitu testaus (11 artikla). Valtioneuvosto katsoo, että jos testauksen on tarkoitus olla pakollista, siitä aiheutuu kuluja toimijoille. Tässä tapauksessa ehdotettua sääntelyä olisi täsmennettävä, jotta se täyttäisi omaisuuden suojan rajoitukselta edellytetyn täsmällisyyden ja tarkkarajaisuuden vaatimukset.

EU:n kyberturvallisuusreservi koostuisi vahvistettujen kriteerien mukaisesti valittujen luotettavien palveluntarjoajien poikkeamienhallintapalveluista (12(1) artikla). Kyberturvallisuusreservi muodostettaisiin ilmeisesti hankintamenettelyn kautta (16(1) artikla). Jäsenvaltiot ja unionin elimet saisivat ilmeisesti käyttää vain reservissä olevia palveluntarjoajia, kun ne reagoivat tai

tukevat reagoimista kriittisten tai erittäin kriittisten alojen toimijoihin vaikuttaviin merkittäviin tai laajamittaisiin poikkeamiin (12(4) artikla). Tämä tarkoittaisi sitä, että vain tietyt toimijat saisivat tarjota kyseisiä palveluita viranomaisille ja unionin elimille. Sinänsä elinkeinovapauden rajoitukselle olisi hyväksyttävä syy eli tavoite varmistaa kyky reagoida vakaviin kyberturvallisuuspoikkeamiin laadukkaiden ulkopuolisten palveluiden avulla. Myös hankintamenettelyn käyttäminen toimijoiden valitsemiseen – kunhan menettely on avoin ja tasapuolinen – vähentää puuttumisen astetta. Valtioneuvosto katsoo, että esitettyä sääntelyä on kuitenkin syytä osin selkeyttää ja tarvittaessa täsmentää (ks. esim. PeVL 60/2001 vp, s. 4/II). Näin on esimerkiksi sen osalta, rinnastuuko menettely luvan- tai ilmoituksenvaraisuuteen (ks. PeVL 69/2014 vp, s. 2/II), onko pätevyysvaatimukset kirjoitettu tarpeeksi tarkasti (vrt. PeVL 8/2005 vp, s. 3) ja onko kyse sidotusta harkinnasta vai tarkoituksenmukaisuusharkinnasta (ks. PeVL 69/2014 vp, s. 2/II).

Valtioneuvosto toteaa, että palveluntarjoajaan kohdistuva sertifiointipakko (16(2)(j)) aiheuttaa palveluntarjoajalle kuluja ja on siten rajoitus tämän omaisuuden suojaan. Valtioneuvosto kuitenkin katsoo, että tämä voidaan perustella samalla hyväksyttävällä syyllä kuin edellä käsitelty elinkeinovapauden rajoitus. Sertifioinnin saamiseen liittyviä vaatimuksia on kuitenkin vielä tarkemmin arvioitava, jotta voidaan varmistua vaatimusten oikeasuhtaisuudesta.

Muuta

Oikeusperustaa ja toimivallan siirtoa on käsitelty edellä niitä koskevissa jaksoissa. Ne ovat EU-oikeudellisia kysymyksiä. Perustuslakivaliokunta on pitänyt kuitenkin tärkeänä, että unionilainsäädäntöä kehitetään ensisijaisesti perussopimusten puitteissa (ks. esim. PeVL 31/2022 vp, 8 kohta). Perustuslakivaliokunta on myös kiinnittänyt huomiota toimivallan siirtoon (ks. esim. PeVL 37/2021 vp, 42 kohta).

7 Ahvenanmaan toimivalta

Kybersolidaarisuusasetuksessa säädettäisiin yhteistyöstä jäsenvaltioiden ja unionin elinten kesken kyberturvallisuuden alalla sekä avun saamisesta kyberreserviin kuuluvilta toimijoilta. Kyberturvallisuusasetukseen ehdotetuilla muutoksilla puolestaan lisättäisiin tietoturvapalveluntarjoajat asetuksen velvoitteiden piiriin ja mahdollistettaisiin niitä koskevan yhteisen sertifiointijärjestelmän luominen. Kyberturvallisuutta ei ole nimenomaisesti mainittu itsehallintolaissa. Näin ollen asiaa on arvioitava maakunnan ja valtakunnan välistä toimivaltajakoa koskevien perusteiden mukaan, jotka osoittavat, mikä kuuluu maakunnalle ja mikä valtakunnalle. Ahvenanmaan itsehallintolain (1144/1991) 27 §:n mukaan valtakunnalla on lainsäädäntövaltaa asioissa, jotka koskevat valtion viranomaisten järjestysmuotoa ja toimintaa (3 kohta) ja teletoimintaa (40 kohta). Sen sijaan itsehallintolain 18 §:n mukaan maakunnalla on lainsäädäntövalta asioissa, jotka koskevat maakunnan hallitusta sekä sen alaisia viranomaisia ja laitoksia (1 kohta). Lainsäädäntövalvonnassa on katsottu, että viranomaisten hallussa olevien asiakirjojen julkisuus ja niiden hallussa olevien henkilötietojen suoja ovat maakunnan lainsäädäntövaltaan kuuluvia asioita.

Valtioneuvosto katsoo, että ehdotettu sääntely kuuluu valtakunnan lainsäädäntövaltaan. Siinä säädetyt asiat rinnastuvat teletoimintaan sekä valtion viranomaisten (Liikenne- ja viestintäviraston Kyberturvallisuuskeskus) toimivaltaan kuuluviin asioihin. Edellä kuvatulla tavalla kybersolidaarisuusasetuksen suhde julkisuus- ja tietosuojasääntelyyn on epäselvä. Valtioneuvoston käsityksen mukaan sääntely ei kuitenkaan vaikuttaisi maakunnan viranomaisten tiedonhallintaan tältä osin, sillä maakunnan viranomaiset eivät osallistuisi yhteistyöhön muutoin kuin mahdollisesti saamalla apua kyberturvallisuusreservistä. Valtioneuvosto toteaa selvyyden vuoksi, ettei ehdotettu kybersolidaarisuusasetus muuta viranomaisten velvollisuutta varautua

kyberuhkiin eikä siten tältä osin muuta maakunnan viranomaisten tiedonhallintaan liittyviä velvollisuuksia.

8 Ehdotuksen käsittely Euroopan unionin toimielimissä ja muiden jäsenvaltioiden kannat

Komissio antoi asetusehdotuksen 18.4.2023.

Ehdotuksen käsittely on alkanut neuvoston horisontaalisessa kybertyöryhmässä 26.4.2023. Ehdotuksen käsittely Euroopan parlamentissa ei ole vielä alkanut.

9 Ehdotuksen kansallinen käsittely

U-kirjelmä on valmisteltu liikenne- ja viestintäministeriössä yhteistyössä valtioneuvoston kanslian, valtiovarainministeriön, oikeusministeriön, työ- ja elinkeinoministeriön, ulkoministeriön, sisäministeriön, puolustusministeriön sekä Liikenne- ja viestintävirasto Traficomin ja Puolustusvoimien kanssa.

Luonnos U-kirjelmäksi on käsitelty viestintäjaostossa (EU-19) 29.5.2023–2.6.2023 ja hybridiuhat ja kriisivarautuminen-jaostossa (EU-13) 29.5.2023–2.6.2023. Lisäksi ehdotuksesta järjestettiin kuulemistilaisuudet viranomaisille 3.5.2023 ja yksityiselle sektorille 8.5.2023.

10 Valtioneuvoston kanta

10.1 Kybersolidaarisuussäädösehdotus

Valtioneuvosto katsoo, että kyberturvallisuus on olennainen osa EU:n sisämarkkinoiden häiriöttömän toiminnan ja yhteiskuntavakauden sekä kansalaisten yksityisyyden turvaamista. Valtioneuvosto kannattaa ehdotetun kybersolidaarisuussäädöksen tavoitteita, mutta toteaa, että aloitteen arvioiduista vaikutuksista ja kustannuksista tarvitaan vielä lisätietoja.

Kyberuhkien osalta valtioneuvosto painottaa yhtenäisen lähestymistavan, tiedonvaihdon ja yhteisen tilannekuvan sekä kriisivasteen tärkeyttä Euroopalle kyberturvallisuushaasteisiin vastaamiseksi. Valtioneuvosto katsoo, että on Suomen edun mukaista vahvistaa kyberturvallisuutta myös EU:n yhteisillä toimilla, ja hakea ja hyödyntää kansallisten ja unionin tason toimien välisiä synergioita. Valtioneuvosto pitää EU:n kriisinkestävyyden kokonaisvaltaista kehittämistä keskeisenä.

Valtioneuvosto kannattaa toimia, jotka edistävät jäsenmaiden välistä tietojenvaihtoa kyberturvallisuuspoikkeamista. Valtioneuvosto kuitenkin toteaa, että uusien tilannekuva- ja tiedonvaihtotoimintojen perustamisessa tulee välttää päällekkäisyyksiä jo olemassa olevien toimintojen kanssa. Valtioneuvosto katsoo, että kansallisten SOC-toimijoiden ja rajat ylittävien SOC-yhteenliittymien välisestä tietojenvaihdosta sekä komissiolle annettavasta toimivallan siirrosta tarvitaan lisätietoja.

Kyberhätätilanteiden mekanismin osalta valtioneuvosto suhtautuu myönteisesti toimiin, joilla pyritään koordinoidusti vahvistamaan kriittisten toimialojen varautumista kyberhäiriötilanteisiin. Valtioneuvosto katsoo, että kriittisten toimijoiden fyysisen ja digitaalista kriisinkestävyyden ja varautumisen edistäminen EU:ssa on erityisen tärkeää.

Kyberturvallisuusreservin osalta valtioneuvosto kannattaa toimia, jotka voivat hidastaa tai ehkäistä merkittävien tai laaja-alaisten kyberhäiriöiden leviämistä. Suhteellisuusperiaate huomioiden, valtioneuvosto pitää tärkeänä, ettei rahoitusinstrumenttien avulla luoda jäsenvaltioille sellaisia kannustimia, jotka heikentävät jäsenmaiden omien kyberturvallisuuskyvykkyyksien kehittämistä. Kyberuhkien rajat ylittävän luonteen vuoksi valtioneuvosto suhtautuu myönteisesti kyberturvallisuusreservin palveluiden ulottamiseen myös kolmansille maille. Valtioneuvosto pitää tärkeänä, että kyberhätätilanteiden mekanismi ja kyberturvallisuusreservi edistävät suomalaisten tietoturva-alan yritysten liiketoimintamahdollisuuksia sisämarkkinoilla.

Valtioneuvosto suhtautuu ehdotettuun kyberpoikkeamien jälkitarkastelumekanismiin lähtökohtaisen myönteisesti, mutta sen toiminnasta, tietojen luovutuksesta ja tietojen vaihdosta tarvitaan lisätietoja. Tiedonvaihtoon, jolla voisi olla negatiivisia vaikutuksia kansalliseen turvallisuuteen, suhtaudutaan varauksellisesti.

Valtioneuvosto näkee Digitaalinen Eurooppa-ohjelman EU:n olennaisena sitoumuksena digitaalisen muutoksen tukemisessa. Etenkin panostukset strategisiin hankkeisiin, kuten tekoälyyn ja kyberturvallisuuteen tukevat EU:n kasvua ja kilpailukykyä. Digitaalinen Eurooppa-ohjelman rahoitukseen kohdistuvien muutosten osalta valtioneuvosto korostaa tarvetta analysoida mahdollisia rahoitusinstrumenttien uudelleen kohdentamisen vaikutuksia niiden alkuperäisiin tarkoituksiin tarkemmin.

Valtioneuvosto suhtautuu varauksellisesti Digitaalinen Eurooppa -ohjelmaan ehdotettuun muutokseen siitä, että käyttämättömien maksusitoumus- ja maksumäärärahojen osalta poikettaisiin varainhoitoasetuksen mukaisesta vuotuisuusperiaatteesta, jonka mukaan käyttämättömät määrärahat peruutetaan varainhoitovuoden päättyessä (ks. U 78/2022 vp varainhoitoasetuksen uudelleenlaadinnasta). Komission ehdottama menettely on erityisen poikkeuksellinen siitä syystä, että varat otettaisiin käyttöön tulevina varainhoitovuosina automaattisesti eikä harkinnanvaraisesti.

Valtioneuvosto katsoo, että unionin tason kyberturvallisuuden operatiiviset tehtävät kuuluisi säilyttää ensisijaisesti Euroopan kyberturvallisuusvirasto ENISAlla. Valtioneuvosto katsoo, että ENISA:n tulisi toiminnassaan välttää päällekkäisyyksiä kansallisten viranomaisten toiminnan kanssa. Valtioneuvosto pitää tärkeänä, että kyberturvallisuuden viranomaisille esitettyjä lisätehtäviä tarkasteltaessa pyritään hillitsemään ehdotuksesta syntyvä hallinnollinen lisätaakka.

Valtioneuvosto katsoo, että ehdotuksen yhteyttä teollisuuteen ja lainsäädännön lähentämiseen tarkennettaisiin huomioiden ehdotuksen oikeusperusta. Valtioneuvosto katsoo, että jatkovalmistelussa on arvioitava erityisesti ehdotuksen suhdetta kansalliseen turvallisuuteen, joka kuuluu yksinomaan kunkin jäsenvaltion vastuulle. Toissijaisuusperiaatteen osalta valtioneuvosto huomauttaa, että kansallisen turvaoperaatiokeskuksen nimeämisessä ei tulisi rajoittaa jäsenvaltioiden hallinnollista autonomiaa.

10.2 Kyberturvallisuusasetukseen ehdotetut muutokset

Valtioneuvosto pitää tärkeänä, että ehdotuksella pyritään vahvistamaan tietoturvallisuutta koko EU:n alueella ja parantamaan tietoturvallisten palveluiden saatavuutta sisämarkkinoilla.

Valtioneuvosto pitää tärkeänä, että tietoturvallisten palveluiden standardointi- ja sertifiointitoiminta hyödyttää suomalaisia yrityksiä, muttei aiheuta niille ylimääräistä, kilpailukykyä haittaavaa hallinnollista taakkaa. Ehdotetun luotettujen palveluntarjoajien sertifiointikehyksen tavoitteita voidaan pitää kannatettava siltä osin kuin sääntelyllä pyrittäisiin lisäämään luottamusta

digitaalisille sisämarkkinoille, vähentämään yrityksille sertifioinnista aiheutuvia kuluja ja parantamaan kyberturvallisuuspalveluiden laatua ja turvallisuutta. Ehdotettujen keinojen ja menettelyiden tehokkuutta suhteessa tavoiteltavaan päämäärään tulee kuitenkin vielä arvioida huolellisesti. Valtioneuvosto pitää tärkeänä, että luotettujen palveluntarjoajien sertifiointi edistää suomalaisten tietoturva-alan yritysten liiketoimintamahdollisuuksia sisämarkkinoilla.