Valtioneuvoston kanslia		PERUSMUISTIO	VNEUS2021-00066
VNEUS	Julkunen Ilona(VNK)	27.01.2021	

Asia

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

Kokous

U/E/UTP-tunnus

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Komissio ja EU:n ulkoasioiden ja turvallisuuspolitiikan korkea edustaja julkaisivat 16.12.2020 tiedonannon EU:n kyberstrategia digitaaliselle vuosikymmenelle (JOIN(2020 18 final).

Tiedonanto on osa niin sanottua komission ja korkean edustajan kyberturvallisuuspakettia, joka sisältää muun muassa ehdotuksen verkko- ja tietoturvadirektiivin päivittämiseksi (COM(2020) 823 final). Komissio on antanut myös lainsäädäntöehdotuksen kriittisten toimijoiden suojelemiseksi (COM(2020) 829 final). Kyberstrategian liitteessä komissio esittää näkemyksensä 5G-verkkojen turvallisuuteen liittyvistä seuraavista askeleista.

Tiedonannon käsittely käynnistyi tammikuussa neuvoston horisontaalisessa kybertyöryhmässä ja puheenjohtajamaan tavoitteena on valmistella asiasta päätelmät, jotka on tarkoitus hyväksyä yleisten asioiden neuvostossa 23.3.2021.

Suomen kanta

Yleistä

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 ennaltaehkäisemiseksi, estämiseksi ja niihin vastaamiseksi. Muun muassa verkko- ja tietoturva-asioista 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:in 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 ennaltaehkäisemiseksi. Yhteisen lähestymistavan pohjalta EU:lla olisi nykyistä paremmat mahdollisuudet edesauttaa sääntöpohjaisuutta, vastuullisen valtiokäyttäytymisen ja kansainvälisen kyberyhteistyön vakiinnuttamista.

Suomi pitää kannatettavana komission ehdotusta pohtia, miten kyberdiplomatian välineistö ja SEU-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 uudet 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 yhteisten 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 ja arkaluonteisten turvallisuusluokittelemattomien tiedon 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.

Pääasiallinen sisältö

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, kvanttilaskennan osalta.

Häiriönsietokyky, teknologinen riippumattomuus ja johtajuus

Infrastruktuurin ja kriittisten palveluiden häiriönsietokyky

Komissio ehdottaa verkko- ja tietoturvadirektiivin päivittämistä kyberresilienssin vahvistamiseksi. Tavoitteena on yhtenäistää sisämarkkinoilla tehtäviä toimia. Lisäksi komissio ehdottaa lainsäädännön päivittämistä kriittisten toimijoiden suojelemiseksi fyysisiltä uhilta. Komissio ilmoittaa myös ehdottavansa rajat ylittävien sähkövirtojen kyberturvallisuutta koskevia toimenpiteitä, joiden tulisi astua voimaan vuoden 2022 loppuun mennessä.
Strategiassa tuodaan myös esiin rahoitussektorille ja lentoliikenteeseen ehdotetut kyberturvallisuutta parantavat toimet. Avaruusohjelman osalta komissio aikoo kehittää Galileo-ohjelman kyberturvallisuusstrategiaa.

EU:n kyberturvallisuusjärjestelyjen kehittäminen

Tiedonvaihdon edistämiseksi ja paremman tilannekuvan saavuttamiseksi strategiassa ehdotetaan tietoturvan valvomopalveluiden verkoston rakentamista**.** Myös nykyisten valvomopalveluiden toimintaa tuettaisiin ja uusia palveluita perustettaisiin. Verkoston avulla voitaisiin tuottaa ajantasaisia varoituksia kyberturvallisuutta uhkaavista tapahtumista viranomaisille ja sidosryhmille.

Strategiassa todetaan, että verkosto voisi sitoutua tukemaan yli 300 miljoonalla eurolla julkisen ja yksityisen sektorin yhteistyötä ja rajat ylittävää yhteistyötä. Komissio kannustaa jäsenmaita osallistumaan tähän yhteissijoitukseen.

Huipputurvallisen viestintäinfrastruktuurin kehittäminen

Avaruusohjelmaan kuuluva EU:n valtiollinen sateliittiviestintäohjelma (Govsatcom) tulee tarjoamaan turvallisia ja kustannustehokkaita avaruusperusteisia viestintävalmiuksia EU:n ja sen jäsenmaiden toteuttamien kriittisten missioiden ja operaatioiden turvaamiseksi. Useimmat jäsenmaat ovat myös sitoutuneet työskentelemään komission kanssa turvallisen kvanttiviestintäinfrastruktuurin (quantum communication infrastructure, QCI) käyttöönoton mahdollistamiseksi Euroopassa. Komissio ilmoittaa jatkossa tarkastelevansa mahdollisuutta ottaa käyttöön monikiertoratainen turvallisten yhteyksien järjestelmä (multi-orbital secure connectivity system).

Seuraavan sukupolven mobiililaajakaistaverkkojen turvaaminen

5G-verkkojen turvallisuuteen liittyen komissio painottaa, että EU:n ja jäsenmaiden tulisi huolehtia, että identifioituja riskejä vähennetään erityisesti liittyen riippuvuuteen korkean riskin palveluntarjoajista. Komissio kannustaa jäsenmaita toimeenpanemaan 5G työkalupakin pääelementit vuoden 2021 toiseen vuosineljännekseen mennessä. Komissio identifioi päätavoitteiksi yhtenäisen kansallisten lähestymistapojen varmistamisen tehokasta riskinhallintaa varten kaikkialla EU:ssa, jatkuvan tiedonvaihdon ja valmiuksien kehittämisen sekä toimitusketjujen resilienssin vahvistamisen.

Tietoturvallisten esineiden Internet

Internettiin kytkettyjen laitteiden osalta komissio viittaa kyberturvallisuusasetuksen puitteissa tehtävään työhön avoimiin turvallisuusratkaisuihin ja sertifiointiin liittyen. Komissio tarkastelee mahdollisuutta laatia horisontaalista lainsäädäntöä internettiin kytkettyjen laitteiden ja niihin liittyvien palveluiden kyberturvallisuuden parantamiseksi. Sääntely voisi sisältää huolellisuusvelvoitteita tuotteiden valmistajille.

Internetin turvallisuuden maailmanlaajuinen parantaminen

Internetin turvallisuuden parantamiseksi komissio aikoo laatia maailmanlaajuisen DNS (domain name system) järjestelmän eheyteen ja saatavuuteen vaikuttavien äärimmäisten skenaarioiden varalta valmiussuunnitelman, jota tuetaan EU:n rahoituksella.

Komissio ilmaisee huolensa DNS- nimipalveluiden markkinoiden keskittymisestä muutamien yritysten käsiin ja tulee tämän vuoksi kannustamaan sidosryhmiä, kuten EU-yrityksiä, Internet-palveluntarjoajia ja selaintoimittajia ottamaan käyttöön DNS-nimipalvelujen monipuolistamisstrategian. Lisäksi komissio tukee julkisen eurooppalaisen DNS-nimipalvelunkehittämistä (’DNS4EU’-aloite).

Yhteistyössä jäsenmaiden ja teollisuuden kanssa komisso aikoo edistää myös IPv6 internetstandardien käyttöönottoa tarvittaessa sääntelyn avulla.

EU:n aseman vahvistaminen teknologian toimitusketjuissa

Komissio näkee, että 2021-2027 rahoituskehyksen avulla voidaan vahvistaa EU:n asemaa teknologian toimitusketjuissa. Julkisen sektorin osalta toimet nojautuvat EU:n julkisia hankintoja koskeva lainsäädäntökehykseen sekä Euroopan yhteistä etua koskevien tärkeiden hankkeiden (IPCEI) puitteissa tehtävään työhön. Myös teknisen tuen väline on tärkeässä asemassa.

Kyberturvallisuuden kompetenssikeskuksen välityksellä tehtävien investointien (erityisesti Digitaalinen Eurooppa-ja Horisontti-Eurooppa-ohjelmien sekä elpymisvälineen) avulla voidaan sijoittaa 4,5 miljardia julkisia ja yksityisiä investointeja vuosien 2021-2027 välillä.

EU:n työvoiman kybertaitojen parantaminen

Komissio kiinnittää myös huomiota EU:n työvoiman kybertaitojen vahvistamiseen. Päivitetty digitaalisen koulutuksen toimintasuunnitelma pyrkii lisäämään tietoisuutta kyberturvallisuudesta ja naisten osallistumista STEM-aloille (luonnontieteet, teknologia, insinööritieteet ja matematiikka).Julkisen ja yksityisen sektorin yhteistyöllä pyritään parantamaan EU:n yritysten kykyä torjua teollis- ja tekijänoikeuksien kybervarkauksia. Kyberturvallisuuden ja –puolustuksen osaamista tulisi myös kehittää.

Operatiivisten valmiuksien kehittäminen uhkien ehkäisemiseksi, torjumiseksi ja niihin vastaamiseksi

Yhteisen kyberyksikön perustaminen

Komissio ja korkeaedustaja julkaisevat helmikuuhun 2021 mennessä prosessikuvauksen yhteisen kyberyksikön perustamisesta. Yksikön perustaminen nähdään tärkeänä askeleena eurooppalaisen kyberturvallisuuden kriisinhallintakehyksen valmiiksi saattamisessa. Kyberyksiköllä olisi kolme päätavoitetta; kyberturvallisuusyhteisöjen valmiusasteen vahvistaminen, yhteisen tilannekuvan muodostaminen ja koordinoidun reaktion mahdollistaminen.

Kyberrikollisuuden torjunta

Kyberrikollisuuden ehkäisemisen osalta komissio tuo esiin tarpeen identifioida ja asettaa kyberrikollisuutta harjoittavat toimijat syytteenalaisiksi. Komissio tukee Europolin ja ENISA:n välistä yhteistyötä ja näkee, että EU-viranomaisten ja kansallisten viranomaisten tulisi laajentaa ja parantaa lainvalvontaviranomaisten valmiuksia kyberrikollisuuden tutkimiseen ottaen samalla huomioon tarve kunnioittaa perusoikeuksia.

Komissio näkee, että kyberrikollisuutta torjuva olemassa oleva lainsäädäntö tulee toimeenpanna tehokkaasti. Erityistä huomiota kiinnitetään lasten seksuaaliseen hyväksikäyttöön verkossa sekä digitaaliseen rikostutkimukseen, mukaan lukien pimeässä verkossa tapahtuvat rikokset. Komissio ilmoittaa julkaisevansa toimintasuunnitelman lainvalvontaviranomaisten digitaalisten valmiuksien parantamiseksi. Sähköisen todistusaineistoa (e-evidence) koskevaa lainsäädäntötyötä jatketaan. Komissio jatkaa työtä lainvalvontaviranomaisten digitaalisen tutkinnan valmiuksien tukemiseksi, mukaan lukien rikostutkinnassa esiintyvän salauksen käsittely.

EU:n kyberdiplomatian työkalupakki

Strategiassa todetaan, että tehokas EU:n diplomaattinen toiminta edellyttää vahvaa yhteistä tilannetietoisuutta ja kykyä valmistella nopeasti EU:n yhteinen kanta. Korkea edustaja tulee edistämään EU:n tiedusteluanalyysikeskukseen (INTCEN) sijoitetun jäsenvaltioiden EU-kybertiedustelua käsittelevän työryhmän perustamista.

Jotta EU voisi paremmin estää, hillitä, ehkäistä ja torjua haitallista kybertoimintaa ja vastata siihen, korkea edustaja ja komissio ilmoittavat antavansa ehdotuksen EU:lle sen kyberpelotetta koskevan kannan määrittelemiseksi tarkemmin. Kyberpelotetta koskevalla kannalla olisi edistettävä valtion vastuullista käyttäytymistä ja yhteistyötä kybertoimintaympäristössä kyberdiplomatian välineistön puitteissa tähän mennessä tehdyn työn pohjalta. Sen kuvataan ohjaavaan erityisesti sellaisten kyberhyökkäysten torjuntaa, joilla on suurin vaikutus, kuten kriittiseen infrastruktuuriin, demokraattisiin instituutioihin ja prosesseihin, sekä toimitusketjuihin kohdistuvien hyökkäysten ja teollis- ja tekijänoikeuksien kybervarkauksien torjunta. Lisäksi kyberpelottetta koskevan kannan tulisi kuvata, kuinka EU ja jäsenmaat voivat parantaa kykyään attribuoida pahantahtoista kybertoimintaa.

Korkea edustaja pyrkii myös yhdessä neuvoston ja komission kanssa tarkastelemaan kyberdiplomatian välineistön lisätoimenpiteitä, mukaan lukien mahdollisuutta uusiin rajoittaviin toimenpiteisiin sekä tarkastelemaan määräenemmistöpäätöksiä kyberhyökkäysten vastaisten horisontaalisten pakotteiden yhteydessä.

Kyberdiplomatiatyökalupakin soveltamista koskevien suuntaviivojen päivittämistä ehdotetaan. Komissio ja korkeaedustaja näkevät, että EU:n tulisi vahvistaa yhteistyötä kansainvälisten kumppaneiden, kuten NATO:n kanssa yhteisen tilannekuvan, yhteistyömekanismien ja diplomaattisten toimien osalta. Strategiassa todetaan, että EU:n kyberdiplomatiavälineistön integroimista EU:n kriisimekanismeihin tulisi edistää. Olisi pyrittävä synergiaan sellaisten toimien kanssa, joita toteutetaan hybridiuhkien torjumista koskevan yhteisen kehyksen ja demokratiaa koskevan

eurooppalaisen toimintasuunnitelman puitteissa hybridiuhkien, disinformaation ja ulkomaisen sekaantumisen torjumiseksi. Strategian mukaan tässä yhteydessä EU:n olisi pohdittava, miten kyberdiplomatian välineistö ja SEU-sopimuksen 42 artiklan 7 kohdan ja SEUT-sopimuksen 222 artiklan mahdollinen käyttö vaikuttavat toisiinsa.

Kyberpuolustusvalmiuksien tehostaminen

Kyberpuolustuksen osalta komissio ja korkeaedustaja näkevät, että EU:n ja jäsenmaiden tulee vahvistaa kykyään ehkäistä ja vastata kyberuhkiin ja tulevat näin ollen tarkastelemaan uudelleen kyberpuolustuksen politiikkakehystä Tämä informoi tulevaa strategiseen kompassiin liittyvää työtä sen varmistamiseksi, että kyberturvallisuus ja kyberpuolustus sisällytetään laajempaan turvallisuus- ja puolustusohjelmaan. EU:n sotilaskomitean tuleva julkaisu, joka käsittelee sotilaallista visiota ja strategiaa kyberavaruudesta toiminnan alueena tulee käsittelemään sitä, kuinka tämä määrittely mahdollistaa EU:n yhteisen turvallisuus ja puolustuspolitiikan sotilasoperaatiot. Myös Euroopan puolustusviraston (EDA) perustama sotilaallinen CERT-verkosto tulee vahvistamaan jäsenmaiden välistä yhteistyötä. Strategiassa kannustetaan jäsenmaita hyödyntämään pysyvän rakenteellisen yhteistyön (PRY) ja Euroopan puolustusrahaston tuomia mahdollisuuksia täysimääräisesti. Komissio ilmoittaa julkaisevansa vuoden 2021 ensimmäisellä neljänneksellä toimintasuunnitelman liittyen siviili-, puolustus- ja avaruusteollisuuden synergioihin.

Globaalin ja avoimen kybertoimintaympäristön edistäminen

EU:n johtoasema kybertoimintaympäristön standardien, normien ja viitekehyksen luomisessa

Strategiassa esitetään, että EU:n on vahvistettava toimintaansa kansainvälisissä standardointiprosesseissa ja parannettava edustustaan kansainvälisissä ja eurooppalaisissa standardointiorganisaatioissa.

Strategia korostaa tarvetta jatkaa työtä kansainvälisten kumppanien kanssa globaalin, avoimen, vakaan ja turvallisen kybertoimintaympäristön edistämiseksi. Kansainvälisen lain, erityisesti YK:n peruskirjan kunnioittaminen on ensiarvoisen tärkeää. Strategiassa esitetään, että EU:n tulisi muodostaa yhteinen kanta kansainvälisen lain soveltamisesta kyberympäristössä.

EU jatkaa niiden kolmansien maiden tukemista, jotka haluavat liittyä Euroopan neuvoston kyberrikollisuutta koskevaan sopimukseen (Budapestin sopimus) ja jatkaa työtä neuvotteluiden loppuun saattamiseksi toisen lisäpöytäkirjan osalta. Strategiassa todetaan, että tarvetta uudelle oikeudelliselle välineelle YK:n piirissä ei ole.

Yhteistyö kumppaneiden ja sidosryhmien kanssa

Strategiassa ehdotetaan, että EU kävisi säännönmukaisia keskusteluja alueellisten organisaatioiden ja epävirallisen EU:n kyberdiplomatian verkoston perustamista EU:n kybertoimintaympäristöä koskevan vision edistämiseksi. Strategiassa ehdotetaan EU-NATO yhteistyön kehittämistä erityisesti kyberpuolustuksen yhteensopivuuskriteereissä. Lisäksi nähdään, että yhteistyötä koulutuksessa ja harjoituksissa tulisi tarkastella.

Strategiassa todetaan, että Internetin hallinnoinnin osalta EU tukee vahvasti useisiin sidosryhmiin perustuvaa lähestymistapaa. Yhdenkään toimijan, hallituksen tai kansainvälisen organisaation ei tulisi pyrkiä kontrolloimaan Internetiä.

EU:n globaalin toimintakyvyn vahvistaminen maailmanlaajuisen häiriönsietokyvyn parantamiseksi

Kansainvälisten kumppaneiden tukemiseksi ehdotetaan EU:n ulkoisten kybervalmiuksien kehittämisohjelman sekä EU:n toimielimien välisen kybervalmiuksien kehittämiskomitean perustamista. Strategiassa ehdotetaan, että toimet kohdistettaisiin erityisesti Länsi-Balkanin ja EU:n naapuruston alueelle sekä kumppanimaihin, joiden digitaalinen kehitys etenee nopeasti.

Kyberturvallisuus EU-instituutioissa, -toimielimissä ja -virastoissa.

EU-instituutiot, -toimielimet ja virastot ovat usein kyberhyökkäysten, erityisesti kybervakoilun, kohteena. EU-toimijoiden kyvyssä havaita ja vastata pahantahtoiseen kybertoimintaan on merkittäviä eroja. Komissio ja korkea edustaja näkevät, että turvallisuusluokitellun sekä luokittelemattoman informaation käsittelyyn tarvitaan yhdenmukainen lähestymistapa instituutioiden välillä. Tämä voisi toimia mallina yhteen toimivuudelle myös jäsenmaiden välillä.
Komissio tulee ehdottamaan vuoden 2021 aikana EU:n instituutioiden, -toimielimien ja virastojen kyberturvallisuutta ja tietoturvaakoskevia yhteisiä sitovia sääntöjä.

Komissio näkee myös tarpeelliseksi CERT-EU järjestelmän mandaatin vahvistamisen.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

Komission ja korkean edustajan yhteinen tiedonanto ei ole oikeudellisesti sitova.

Käsittely Euroopan parlamentissa

Euroopan parlamentissa vastuuvaliokunta on ITRE (teollisuus, tutkimus ja energia).
Parlamenttikäsittelystä ei ole vielä saatavilla tietoa.

Kansallinen valmistelu

VNK:n koordinoima E-kirje on laadittu yhteistyössä ministeriöiden (LVM, TEM, UM, PLM, OM, SM ja OKM) kanssa.

E-jatkokirjelmää on käsitelty seuraavien jaostojen kirjallisessa menettelyssä 25.-26.1. 2021:

Viestintäjaosto (EU19)
Oikeus- ja sisäasiat (EU7)
Ulkosuhdejaosto (EU3)

Eduskuntakäsittely

Valtioneuvoston E-selvitys E 83/2017 vp: EU-kybertiedonanto: Resilienssi, pelote ja puolustus

Valtioneuvoston E-selvitys E 16/2013 Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö”

Valtioneuvoston selvitys E-96/2017 vp, EJ 22/2018 vp, EU:n kehittäminen; institutionaaliset kysymykset; päätöksenteon tehostaminen EU:n yhteisessä ulko- ja turvallisuuspolitiikassa.

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

Toimivallanjako EU-asioissa valtakunnan ja Ahvenanmaan välillä määräytyy Ahvenanmaan itsehallintolain (1144/1994) mukaan. Ahvenanmaan asemaa arvioidaan tarvittavilta osin tiedonannossa ehdotettujen toimenpiteiden edetessä.

Tiedonannossa esitetään toimenpide-ehdotuksia. Toimenpiteiden mahdollisia lainsäädännöllisiä vaikutuksia arvioidaan erikseen osana niiden valmistelua.

Taloudelliset vaikutukset

Tiedonannossa esitetään toimenpide-ehdotuksia, joilla toteutuessaan on taloudellisia vaikutuksia sekä EU:n että kansallisen budjetin osalta. Näitä vaikutuksia arvioidaan erikseen osana kunkin aloitteen valmistelua.

Muut asian käsittelyyn vaikuttavat tekijät

Kyberstrategian julkaisemisen yhteydessä komissio julkaisi ehdotuksen verkko- ja tietoturvadirektiivin päivittämiseksi (COM(2020) 823 final) sekä lainsäädäntöehdotuksen kriittisten toimijoiden suojelemiseksi (COM(2020) 829 final).

Kansallisia linjauksia:

Vuoden 2019 kyberturvallisuusstrategia: strategiassa on asetettu keskeisimmät kansalliset tavoitteet kybertoimintaympäristön kehittämiseksi ja siihen liittyvien elintärkeiden toimintojen turvaamiseksi (https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia-2019/)

Vuoden 2020 ulko- ja turvallisuuspoliittinen selonteko**:** Hallituskausittain laadittavassa selonteossa arvioidaan Suomen ulko- ja turvallisuuspoliittista toimintaympäristöä ja määritellään Suomen toiminnan tavoitteet ja painopisteet lähivuosille (http://urn.fi/URN:ISBN:978-952-287-876-2).

Asiakirjat

Korkean edustajan ja komission yhteinen tiedonanto ’EU:n kyberstrategia digitaaliselle vuosikymmenelle’ (JOIN(2020) 18 final)

Laatijan ja muiden käsittelijöiden yhteystiedot

Ilona Julkunen, VNK ilona.julkunen@vnk.fi puh. 0505058869
Erica Karppinen, LVM erica.karppinen@lvm.fi puh. 0295 342 107
Jouko Huhtamäki, SM jouko.huhtamaki@intermin.fi. p. 040 836 6714
Niko Mäkilä, VM, niko.makila@vm.fi, puh. 0295 530 188
Tuija Kuusisto, VM, tuija.kuusisto@vm.fi puh. 0407508330
Stefan Lee, UM, stefan.lee@um.fi puh. 0505558435
Pentti Olin, PLM, pentti.olin@defmin.fi puh. 0504728390
Ilmari Uljas PLM; ilmari.uljas@defmin.fi 050114832
Antti Eskola, TEM, antti.eskola@tem.fi puh. 0503697612
Jonna Korhonen, OKM, jonna.korhonen@minedu.fi 0504779667
Joni Korpinen, OM, joni.korpinen@om.fi 0504387972

EUTORI-tunnus

Liitteet

Viite

Asiasanat	kyberstrategia
Hoitaa	**LVM, OM, PLM, SM, UM, VNK**
Tiedoksi	EUE, OKM, STM, TEM, TULLI, VM, VTV