Liikenne- ja viestintäministeriö NEUVOSTORAPORTTI LVM2022-00118

KAN Kopra Kaisa(LVM) 11.03.2022
JjulkinenJULKINEN

Asia
Epävirallinen televiestintäministerien kokous 8.-9.3.2022

Kokous
Epävirallinen viestintäministerikokous 08.03.2022 - 09.03.2022

Televiestintäministerien epävirallisessa kokouksessa keskusteltiin EU:n kyberturvallisuuden ja operatiivisen valmiustason vahvistamisesta edelleen Ukrainan sodan epävakaassa geopoliittisessa tilanteessa. Ministerit ottivat kantaa ja tukivat EU:n kyberturvallisuuden sääntelykehyksen, hallintorakenteen ja ekosysteemin kehittämistä.

Sisämarkkinakomissaari Breton visio puheessaan Euroopan kyberturvallisuus kilpeä (European Cyber Shield), joka rakentuu neljän pilarin varaan: 1) kyvykkyydet havaita ja tunnistaa kyberuhkia, 2) EU:n kyberturvallisuuskysymysten rakenteet, 3) solidaarisuus jäsenmaiden kesken, sekä 4) EU:n sisäinen resilienssi ja lainsäädäntökehys.

EU:n kyberturvallisuusviraston ENISA pääjohtaja Lepassaar antoi tukensa KOM strategiselle visiolle. ENISA tukee jäsenvaltioita kyberkyvykkyyksien kehittämisessä. Ranskan kyberturvallisuusvirasto ANSSI pääjohtaja Poupard painotti kyberhyökkäysten ennaltaehkäisyä sekä luottamuksen luomista sertifioinnin ja sääntelyn kautta.

Jäsenvaltiot jakoivat yhteisen tilannekuvan Ukrainan sodan vaikutuksesta EU:n kyberturvallisuuteen ja tarpeesta reagoida kyberhyökkäysten uhkaan sekä julkisella että yksityisellä sektorilla. Jäsenvaltiot tukivat lähes yksimielisesti KOM esityksiä EU:n kybervalmiuksien kehittämiseksi. Suomi korosti puheenvuorossaan EU:n yhteisen tilannekuvatyön kehittämistä eri kyberturvallisuustoimijoiden välisen tiedonvaihdon kautta sekä piti tärkeänä kyberharjoituksia valmiuksien testaamiseksi. Lisäksi Suomi painotti Euroopan kyberturvallisuusteollisuuden, teknologioiden ja palveluiden vahvistamista.

Epävirallisessa televiestintäministerien kokouksessa annettiin yhteisaloite EU:n kyberturvallisuuden suorituskykyjen kehittämisestä, mikä sisälsi aloitteen eurooppalaisen kyberturvallisuuden hätärahaston perustamiseksi. Lisäksi kokouksessa annettiin ministerien yhteisvetoomus digiyrityksille disinformaation torjumiseksi verkossa erityisesti Ukrainan sodan kontekstissa.

EU:n kyberturvallisuuden resilienssin ja operatiivisen valmiustason vahvistaminen

Televiestintäministerien politiikkakeskustelu käytiin Euroopan kyberavaruudensuojelemisesta neuvoston puheenjohtajamaa Ranskan tausta-asiakirjassa esitettyjen keskustelukysymysten pohjalta. Ministerit keskustelivat siitä, kuinka EU:n sääntelykehyksessä voitaisiin paremmin ottaa huomioon sisämarkkinoiden suojelu lisääntyviltä kyberhyökkäyksiltä erityisesti epävakaassa geopoliittisessa tilanteessa. Lisäksi ministerit toivat esille konkreettisia ehdotuksia EU:n kyberturvallisuuden ekosysteemin vahvistamiseksi ja EU:n valmiustason nostamiseksi laaja-alaisissa kyberhyökkäyksissä.

Keskusteluun osallistuivat televiestintäministerien lisäksi sisämarkkinakomissaari **Thierry Breton**, EU:n kyberturvallisuusviraston ENISA:n pääjohtaja **Juhan Lepassaar** ja Ranskan kyberturvallisuusvirasto ANSSI:n pääjohtaja **Guillaume Poupard**.

Komissaari Breton kiitti puheenjohtajamaata alustuspuheenvuorossaan tämän tekemästä agendamuutoksesta, joka huomioi Ukrainan sodan vaikutukset kybersektorilla. EU on tehnyt kovia päätöksiä ja toimia Venäjän aggressioon vastaamiseksi. Myös kyberpuolustuksen osalta tarvitaan toimia. KOM katsoi, että EU:n on edelleen kehitettävä valmiuksia vastata laaja-alaisiin kyberhyökkäyksiin ja lisättävä sisäistä koordinaatiota sekä rakennettava eurooppalaisen kyberpuolustuksen kilpi, joka turvaa Eurooppaa kyberturvallisuuden saralla samalla tavalla kuin esimerkiksi Frontex rajaturvallisuudessa. KOM painotti puheenvuorossaan tarvetta kehittää 1) EU:n valmiuksia kyberuhkien havainnoinnissa ja tunnistamisessa, 2) kyberturvallisuuskysymysten hallintaa (governance) operatiivisella, strategisella ja poliittisella tasolla, 3) solidaarisuutta jäsenvaltioiden kesken niin sisäisesti kuin ulkoisesti ja 4) sisämarkkinoiden resilienssiä ml. pk-yritykset sekä tehokasta lainsäädäntökehystä.

Kyberpoikkeamien havainnointiaikaa tulee merkittävästi vähentää vielä nykyisestä mm. teknologioita hyödyntämällä. KOM esittää yhtenä toimena EU:n ja kansallisten kyberturvallisuuden keskitettyjen valvomotoimintojen (SOC - Security Operations Centres) yhteistyön kehittämistä ja yhteisten alustojen rakentamista.

KOM painotti myös EU:n kyberturvallisuuden hallintorakenteen suoraviivaistamista ja yhteistyötä eri sektoreiden välillä. EU:n jäsenvaltioiden välinen kansallisten kyberturvallisuuskeskusten CSIRT-verkosto ja jäsenmaiden kyberturvallisuuskeskusten johtajien CyCLONe-verkosto tekevät hyvää työtä. Eri hallinnonalojen toimijoita ja komiteoita on kuitenkin vielä paljon ja näiden välistä tiedonvaihtoa tulee vielä tehostaa entisestään. Samoin jäsenmaissa vastuu ja koordinaatio kyberturvallisuudessa on usein jakautunut eri ministeriöiden välillä. Yhteistyön tehostamiseksi ja tiedonvaihdon sujuvoittamiseksi KOM on antanut ehdotuksen yhteisen kyberturvallisuusyksikön (JCU) perustamisesta. KOM toivoo esityksen saavan jäsenmaiden poliittisen tuen, aina päämiehiä myöten.

KOM painotti solidaarisuutta jäsenvaltioiden välillä. KOM viittasi EU:n turvallisuus- ja puolustusyhteistyön strategiseen kompassiin, jossa tunnistetaan siviili- ja sotilaalliset yhtymäkohdat. EU tarvitsee myös kyberpuolustuksessa nopean toiminnan joukkoja. Lisäksi jäsenvaltiot tarvitsevat resursseja ja rahoitusta, joista mainittu myös puheenjohtajamaan valmistelemassa televiestintäministerien yhteisaloitteessa kyberkyvykkyyksien kehittämiseksi.

KOM korosti tarvetta EU:n sisämarkkinoiden kyberresilienssin vahvistamiseen. NIS2 verkko- ja tietoturvadirektiivin päivitystä koskevat trilogineuvottelut EP:n kanssa tulisi saattaa päätökseen nopeasti ja direktiivi viedä jäsenmaissa täytäntöön mahdollisimman pian. KOM jatkaa kyberresilienssisäädöksen (Cyber Resilience Act CRA) ehdotuksen valmistelua, joka on odotettavissa syyskuussa 2022. CRA tulee sisältämään velvoitteita IoT-laitteiden, prosessien ja palveluiden osalta kyberturvallisuuden tason nostamiseksi.

ENISA pääjohtaja Juhan Lepassaar antoi tukensa KOM strategiselle visiolle ja ENISA pyrkii sitä mandaattinsa puitteissa edistämään. ENISA tukee jäsenvaltioita NIS2-direktiivin täytäntöönpanossa sekä tukee jäsenvaltioita kyberkyvykkyyksien kehittämisessä. Kesään mennessä ENISA tulee valmistelemaan kyberturvallisuusasetuksen (CSA) mukaisen pilvipalveluiden kyberturvallisuussertifioinnin puitteet. ENISA painottaa julkisen ja yksityisen sektorin yhteistyötä sekä tukee KOM esitystä EU ja kansallisen tason SOC-yhteistyön kehittämisestä. Yhteiskunnan kriittisten sektoreiden resilienssin vahvistamiseksi CSIRT ja CyCLONe –verkostot muodostavat yhteyspisteen, mitä kautta tieto kulkeutuu eri sektoreille. Ehdotetun kyberturvallisuuden hätärahaston osalta ENISA valmistelee ehdotuksia haavoittuvuuksien tunnistamiseksi ja järjestelmien testaamiseksi kriittisillä sektoreilla yhdessä luotettavien eurooppalaisten palveluntoimittajien kanssa.

ANSSI pääjohtaja Guillaume Poupard totesi vakavien kyberhyökkäysten lisääntyneen Ranskassa ja trendi on kasvava. Pk-yrityksiin kohdistuneet hyökkäykset ovat myös lisääntyneet. On tärkeää keskittyä kyberturvallisuudessa ennaltaehkäisyyn ja EU-tasolla osaamisen kehittämiseen sekä sertifioinnin ja sääntelyn kautta luottamuksen vahvistamiseen. ANSSI painotti koordinaatiota yllä mainituissa EU:n kyberturvallisuuden verkostoissa ja hyvää yhteistyötä ENISA ja komission digitaalisuudesta vastaavan pääosaston (DG Connect) kanssa. Digipalveluita tarjoavat yritykset ja teleoperaattorit ovat kriittisiä, sillä niihin kohdistuvien kyberhyökkäysten vaikutukset voivat olla merkittäviä laajasti eri sektoreilla. Lisäksi KOM esille nostama kyberkilpi poikkeaa perinteisistä turvallisuusratkaisuista siinä, että kyberkilvessä kaikkien meidän toimenpiteitä tarvitaan suojan vahvistamiseksi.

Jäsenvaltiot jakoivat yhteisen tilannekuvan Ukrainan sodan vaikutuksesta EU:n kyberturvallisuuteen ja tarpeesta varautua sekä julkisella että yksityisellä sektorilla sekä tehdä päätöksiä EU-tasolla kyberturvallisuuden sääntelykehyksen, hallinnon ja ekosysteemin kehittämiseksi. Jäsenvaltiot tukivat laajasti KOM esityksiä ja ENISA aloitteita. NIS2-direktiivin nopea hyväksyntä ja toimeenpano sai vahvan tuen. Samoin KOM esitys kansallisten ja EU-tason SOC-toimijoiden yhteistyön kehittämisestä. Monessa puheenvuorossa korostettiin olemassa olevan sääntelyn toimenpanoa (CSA, NIS2, 5G toolbox). Jäsenvaltiot painottivat tulevan kyberresilienssiehdotuksen (CRA) tärkeyttä ja katsoivat, että asetuksessa tarvitaan holistista ja internetiin kytketyn laitteen, prosessin tai palvelun koko elinkaaren kattavaa lähestymistapaa. CRA tulisi täydentää ja olla linjassa kyberturvallisuusasetuksen ja NIS2-direktiivin kanssa.

Jäsenvaltiot kiinnittivät huomiota toimitusketjujen kokonaisturvallisuuteen ja vain luotettavien toimittajien käyttämiseen myös niiden tuotteiden tai palveluiden osalta, jotka tulevat EU:n rajojen ulkopuolelta. Kyberturvallisuuden merkitys nousi esille myös Euroopan talouskasvun ja teknologisen suvereniteetin ja omavaraisuuden näkökulmasta. Julkisen ja yksityisen sektorin yhteistyötä pidettiin tärkeänä ekosysteemin kehittämiseksi. Kyberstandardisoinnissa täytyy osallistaa yrityksiä ja erityisesti pk-yritysten kyberturvallisuuden lisäämistä tulee tukea (esim. Digitaalinen Eurooppa -ohjelmasta).

Monessa jäsenvaltioiden puheenvuorossa korostettiin lisäksi EU:n tiedonkulun kanavien kyberturvallisuutta sekä EU:n instituutioiden ja virastojen tietoturvan vahvistamista. Lisäksi pidettiin tärkeänä kokonaisvaltaista ja integroitua lähestymistapaa kyberturvallisuuteen Euroopassa ilman rajanvetoa sisäisen ja ulkoisen turvallisuuden tai kyber- ja digisektoreiden välillä. Myös hallinnonalojen väliset siilot tulisi poistaa, sillä yhdellä sektorilla tapahtunut hyökkäys vaikuttaa toisella sektorilla. Strategista yhteistyötä kaikkien eri toimijoiden välillä ja kaikilla eri tasoilla (operatiivinen, strateginen ja poliittinen) peräänkuulutettiin. Samoin vahvempaa hallintorakennetta ja koordinaatiota eri toimijoiden välillä korostettiin.

Yhteinen kyberturvallisuusyksikkö (JCU) voisi koordinoida EU-tason toimenpiteitä, EU:n nopean toiminnan joukkoja ja kansallisten asiantuntijatiimien työtä sekä tiedonkulkua eri kyberyhteisöjen

välillä. JCU toimenkuvaan tulee identifioida tehtäviä ilman päällekkäisyyksiä olemassa olevien toimijoiden kanssa. CSIRT ja CyCLONe -verkostojen toimintaa arvostettiin laajasti jäsenvaltioiden puheenvuoroissa. Jäsenvaltiot korostivat yhteisten kyberharjoitusten merkitystä ja niistä saatujen oppien toimeenpanoa. Kyberasiantuntijavajeesta johtuen tarvitaan yhteistyötä ja solidaarisuutta jäsenmaiden välillä. EU:n kyberturvallisuuden kompetenssikeskuksen tuleva rooli kyvykkyyksien kasvattamisessa nousi jäsenvaltioiden puheenvuoroissa esille ja tavoitteena olisi saada kompetenssikeskus pian operationaaliseksi.

Lisäksi useat jäsenvaltiot nostivat esille NATO-yhteistyön, transatlanttisen yhteistyön ja globaalin yhteistyön samanmielisten maiden kanssa ml. kyberdiplomatian työkalupakin toimeenpano. Muutama jäsenvaltio nosti esille komission ja jäsenvaltioiden rahoituksen ja investointien lisäämisen kyberturvallisuuteen ja kyberpuolustukseen.

Suomi korosti puheenvuorossaan EU:n yhteisen tilannekuvatyön kehittämistä eri kyberturvallisuustoimijoiden välisen tiedonvaihdon kautta. CyCLONe-verkosto nähdään hyödyllisenä siltana teknisen ja poliittisen tason välillä EU:n kyberturvahallinnassa. Myös yhteistyötä yksityisen sektorin kanssa painotettiin. Kyberharjoitukset ovat tärkeitä yhteistyön ja valmiuksien harjoittelemiseksi laaja-alaisissa kyberhyökkäyksissä. Lisäksi Suomi painotti Euroopan kyberturvallisuusteollisuuden, teknologioiden ja palveluiden vahvistamista, jotta kyberturvallisuusratkaisuja ei tarvitsisi tuoda markkinoille EU:n ulkopuolelta.

Loppupuheenvuorossaan KOM painotti Euroopan kyberturvallisuuden kilven tarvitsevan hallintorakenteen toimiakseen. Breton kiitti laajasta tuesta KOM aloitteille ja totesi, että on tärkeää viedä ehdotettuja aloitteita eteenpäin yhteiskuntien ja kansalaisten suojelemiseksi. KOM palaa SOC-verkostoa koskevaan aloitteeseen ja pyrkii vahvistamaan yhteistyötä kyberpuolustuksessa. Vaikka eri maissa eri ministeriöt vastaavat kyber- ja puolustuskysymyksistä, täytyy meidän työskennellä yhdessä, sillä kyberin ja puolustuksen välillä ei ole rajalinjaa. Myös pk-yritysten resilienssiä on vahvistettava (NIS2) ja tarvitaan myös rahoitusta, sillä luotettava toimittaja ei ole aina halvin. EU:n uusi kyberturvallisuuden hätärahasto olisi solidaarisuusmekanismi, josta voitaisiin tukea jäsenmaita laajan kyberhyökkäyksen tilanteissa. KOM tulee jatkamaan rahaston valmistelua.

Puheenjohtajamaa Ranska kiitti lopuksi KOM esityksistä ja totesi puheenjohtajan tekevän kaikkensa ratkaisujen löytämiseksi kyberturvallisuuden vahvistamiseksi näiden esitysten pohjalta. Puheenjohtajamaa kertoi myös tavoittelevansa kompromissia EP kanssa mahdollisimman pian NIS2 direktiivistä, ja katsoi sen olevan keskeinen säädös Euroopan kyberturvallisuudelle.

Televiestintäministerien epävirallisen kokouksen yhteydessä annettiin televiestintäministerien yhteisaloite EU:n kyberturvallisuuden suorituskykyjen kehittämisestä. Aloitteen keskeisiä tavoitteita on muun muassa kiirehtiä NIS2-direktiivin hyväksymistä ja tulevan kyberresilienssiasetusehdotuksen julkaisua. Aloitteessa halutaan vahvistaa EU yhteistyötä ja solidaarisuutta ja lisätä investointeja eurooppalaisiin kyberturvapalveluiden tarjoajiin. Aloite sisältää myös viittauksen kyberturvallisuuden hätärahastoon ja siinä kiinnitetään huomiota EU:n instituutioiden ja virastojen kyberturvaan.

Muut asiat:

Työlounaalla televiestintäministerit keskustelivat hybridisodankäynnin haasteista yhdessä suurten alustayhtiöiden edustajien kanssa (Google, YouTube, Meta ja Twitter). Agendalla oli erityisesti keinot torjua disinformaatiota ja informaatiovaikuttamista verkossa. Epävirallisen televiestintäministerikokouksen yhteydessä annettiin ministerien yhteisvetoomus digiyrityksille, jossa kehotetaan alustayhtiöitä, sosiaalisen median palveluita, välityspalveluita ja muita tiedonvälityspalveluita estämään disinformaation leviäminen erityisesti Ukrainan sodan kontekstissa.

Digiyritysten tulisi tehdä toimia, joilla varmistetaan, ettei palveluja käytetä vihamielisten sisältöjen ja disinformaation levittämiseen sekä priorisoimaan luotettavia tiedonlähteitä alustoillaan. Yrityksiä kehotetaan myös liittymään ja toimeenpanemaan yritysten itsesääntelyohje (*Code of Practice on Disinformation)*.

Televiestintäministerit keskustelivat lisäksi suljetussa työosiossaan Euroopan sähköisen viestinnän infrastruktuurin ja verkkojen resilienssistä.

Kansainvälisenä naistenpäivänä 8.3. hyväksyttiin myös televiestintäministerien julistus *Nevers Declaration for Women in Entrepreneurship and Innovation*, joka keskittyy naisten yrittäjyyteen, innovointiin ja yritysrahoituksessa olevan sukupuolikuilun kuromiseen ICT-sektorilla.

Suomen edustajat

Ministeri Harakka, erityisavustaja Tino Aalto (LVM), johtava asiantuntija Nina Hyvärinen (LVM), erityisasiantuntija Kaisa Kopra (LVM)

Asiakirjat

Liitteet

Viite

Asiasanat	datatalous, digitalisaatio, hybridiuhat, jaosto hybridiuhat (EU 13), kriittinen infrastruktuuri, kyber, kyberstrategia, liikenne-, televiestintä- ja energianeuvosto, sähköinen viestintä, tietoliikennepalvelut, tietoliikenneverkot, Ukraina, jaosto viestintä (EU 19)
Hoitaa	**LVM, OM, PLM, SM, TEM, UM, VNK**
Tiedoksi	ALR, EUE, LIIVI, MMM, OKM, SP, STM, TULLI, VM, VTV, YM