Liikenne- ja viestintäministeriö Neuvostoraportti EU/10/2025-LVM-8

Lepistö Petri 10.3.2025

Epävirallinen EU-televiestintäministerikokous (kyberturvallisuus) 4.-5.3.2025 Varsova

Kokous

Epävirallinen EU-televiestintäministerikokous 4.-5.3.2025

EU-puheenjohtajamaa Puolan Varsovassa järjestämässä televiestintäministerien epävirallisessa kokouksessa 4.-5.3.2025 oli aiheena kyberturvallisuus. Keskustelua käytiin EU:n yhteistoiminnasta ja reagoinnista kyberturvallisuuden häiriötilanteisiin sekä unionin toimintamallin päivityksestä koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (ns. Kyberturvallisuuden Blueprint). Lisäksi ministerit keskustelivat siviili-sotilasyhteistyöstä kyberturvallisuudessa sekä investoinneista kyberturvallisuuteen. Kokouksen yhteydessä kaikki EU:n jäsenvaltiot antoivat myös ”Warsaw Call on Cybersecurity Challenges” -yhteisjulistuksen ei-sitovista toimista kyberturvallisuuden vahvistamiseksi EU:ssa.

Jäsenmaat korostivat, että kyberturvallisuuden parantamiseksi on tärkeämpää toimeenpanna tehokkaasti jo olemassa olevia rakenteita, lainsäädäntöä ja tehostaa tiedonvaihtoa, lisätä siviili-sotilasyhteistyötä ja synergioita Naton kanssa, sen sijaan että luotaisiin uusia päällekkäisiä mekanismeja. Lisäksi korostettiin digitaalisen suvereniteetin merkitystä ja tarvetta turvata Eurooppaan sijoittautumista tukevan rahoituksen saatavuus kyberturvallisuuden kannalta keskeisten investointien koko elinkaaren ajan perustutkimuksesta aina kaupallistamiseen saakka.

Kyberturvallisuudesta vastaavat ministerit kokoontuivat Puolan puheenjohtajakauden epäviralliseen televiestintäministerikokoukseen Varsovaan 4.-5.3.2025. Suomea edusti liikenne- ja viestintäministeri Lulu Ranne. Epävirallisen kokouksen aiheena oli Puolan turvallisuusteeman prioriteetteja mukaillen kyberturvallisuus. Ministereillä oli kokouksessa kolme keskustelua. Ensimmäisessä sessiossa ministerit keskustelevat EU:n yhteistoiminnasta ja reagoinnista kyberturvallisuuden häiriötilanteisiin sekä unionin toimintamallin päivityksestä koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin (ns. Kyberturvallisuuden Blueprint). Työlounaalla ministerit keskustelivat siviili-sotilasyhteistyöstä kyberturvallisuudessa ja kolmannen keskustelun aiheena oli investoinnit kyberturvallisuuteen.

Komission johtava varapuheenjohtaja Virkkunen totesi puheenvuoroissaan, että Eurooppa on kohdannut yhä laajamittaisempia kyberhyökkäyksiä eri sektoreilla sekä samalla fyysiset iskut kriittistä infrastruktuuria kohtaan ovat lisääntyneet. Tämän takia resilienssin lisääminen kyberturvallisuudessa (mm. Blueprintin päivitys kesäkuussa 2025; NIS2 tehokas implementointi jäsenmaissa) ja kriittisen infrastruktuurin suojaamisessa (mm. *Joint Action Plan on Cable Security*) ovat korkealla komission prioriteettilistalla. Ennaltaehkäisevät toimet, varautuminen äärimmäisiin uhkakuviin, tiiviimpi yhteistyö ja yhteisharjoitukset ovat avainasemassa hyökkäyksiltä suojautumisessa. Samalla Virkkunen kuitenkin toteaa, että näiden toimien toteuttamiseen tarvitaan lisää luottamusta EU-jäsenvaltion välillä sekä kattavat turvalliset viestintäyhteydet, jotta informaatiota voidaan vaihtaa reaaliaikaisesti eri toimijoiden välillä.

Komissio pyrkii aktiivisesti löytämään kokonaisvaltaisia ratkaisuja ja vahvistamaan kyberturvallisuuden

horisontaalia asetelmaa mm. tulevissa EU:n puolustuksen valkoisessa kirjassa, sisäisen turvallisuuden strategiassa ja varautumisunioni strategiassa. Lisäksi komissio kannustaa kehitettäväksi alueellisia rajat ylittäviä kyberkeskuksia (*cross-border cyber hubs*), joiden perustamista EU tukee jopa 75 %:n rahoituksella. KOM DG Roberto Viola toteaa EU:n olevan takamatkalla kaupallisten kyberturvallisuushyödykkeiden markkinassa (75 % kyberturvallisuusratkaistuista tulee muualta), mutta samalla KOM näkee, että EU:n rahoituksen avulla, ENISAn roolin vahvistamisella, ulkoisten riippuvuussuhteiden vähentämisellä esimerkiksi hankintojen kautta, sekä suurilla yhteisprojekteilla, kuten supertietokoneiden avulla EU pystyy nopeasti kehittämään strategista autonomiaa sektorille.

Jäsenmaat jakoivat laajasti näkemyksen siitä, että nyt on tärkeää keskittyä toimeenpanemaan tehokkaasti tuoreessa EU-lainsäädännössä määriteltyjä yhteistyörakenteita, -mekanismeja ja tiedonvaihtoa kyberturvallisuuden hallitsemiseksi unionissa, pikemminkin kuin luomaan uusia päällekkäisiä rakenteita. CSIRT-verkosto (*Computer Security Incident Response Teams*) ja CyCLONe -verkosto (*European Cyber Crisis Liaison Organisation Network*) nähtiin keskeisiä mekanismeina, jotka mahdollistavat tehokkaan koordinoinnin, tietojen vaihtamisen ja reagoinnin kyberuhkiin. Jäsenmaat korostivat tarvetta hyödyntää näitä rakenteita täysimääräisesti, jotta EU voi vahvistaa kollektiivista kyberresilienssiään ilman hallinnollista taakkaa tai toimivaltuuksien hajauttamista. Usea jäsenmaa tuki siviili-sotilasyhteistyön lisäämistä sekä synergioiden löytämistä Naton kanssa. Muutama jäsenmaa nosti puheissaan esiin myös Europolissa omaksutun tapaisen yhteistyön keinona tehostaa ENISAn toimintaa. Jäsenmaat korostivat myös laajasti digitaalisen suvereniteetin merkitystä kyberturvallisuuden vahvistamisessa. Tässä yhteydessä pidettiin erityisen tärkeänä varmistaa Eurooppaan sijoittautumista tukevan rahoituksen saatavuus kyberturvallisuuden kannalta keskeisten investointien koko elinkaaren ajan. Tämä kattaa investointien kaikki vaiheet perustutkimuksesta ja tuotekehityksestä aina kaupallistamiseen ja markkinoille saattamiseen sekä kasvuvaiheisiin asti.

Suomi korosti kokouksessa kriisivalmiuden ja digitaalisen resilienssin tärkeyttä nykyisessä haastavassa geopoliittisessa tilanteessa. Erityisesti kyberturvallisuudessa tarvitaan selkeitä toimintamalleja, vahvaa julkisen ja yksityisen sektorin yhteistyötä sekä tehokasta rajat ylittävää koordinaatiota. Suomi pitää hyvänä komission ehdotusta päivittää EU:n kyberturvallisuuden Blueprint. Kyberturvallisuuden yhteisharjoitukset sekä EU:n sisällä että Naton kanssa ovat välttämättömiä toimijoiden välisen yhteistyön vahvistamiseksi. Lisäksi Suomi korosti vahvaa osaamistaan ja kokemustaan kyberharjoittelusta eri tasoilla, yksityisen sektorin roolin tärkeyttä ja sektorien välistä yhteistyötä julkisen sektorin kanssa. Lisäksi siviili-sotilasyhteistyötä kyberturvallisuudessa on lisättävä.

Suomi katsoi myös, että EU-tason yhteistyömekanismeja tulee vahvistaa edelleen ja syventää yhteistyötä keskeisten kumppanimaiden kuten USA:n ja Iso-Britannia kanssa. EU:n seuraavassa monivuotisessa rahoituskehyksessä on kasvatettava merkittävästi puolustuksen ja kriisivalmiuden rahoitusosuutta sekä panostettava digitaalisiin huipputeknologioihin, kuten tekoälyyn, 5G- ja 6G-teknologiaan, kvanttilaskentaan ja kvanttilaskennan kestävään kryptografiaan. Innovaatiorahoituksen saatavuuden parantaminen sekä digitaalisen osaamisen kehittäminen ovat välttämättömiä Euroopan strategisen kilpailukyvyn vahvistamiseksi.

Puheenjohtaja totesi yhteenvedossaan kokouksen olleen hyvin konsensuspohjainen. EU:n kyberturvallisuuden vahvistamisessa keskeistä on päivittää kyberturvallisuuden Blueprint vastaamaan nykypäivän tilannekuvaa ja selkeyttää toimenpiteet ja roolit eri toimijoiden kesken. Samalla tulee vahvistaa luottamusta jäsenmaiden keskuudessa, luoda turvalliset kommunikointiverkot reaaliaikaiseen informaation jakamiseen sekä tukea ENISA:n toimintaa entistä vahvemmin. Kyberinvestointien lisääminen on kriittisen tärkeää, jotta Eurooppa voi varmistaa riittävät osaamiset ja valmiudet. Lisäksi on vahvistettava julkisia hankintoja, jotta kyberturvallisuuteen liittyvät innovaatiot saadaan tehokkaasti käyttöön. Seuraavana askeleena puheenjohtaja näkee Blueprintin hyväksymisen suunnitellusti televiestintäneuvostossa 6.6.2025, jonka jälkeen EU:n valmiutta tulee testata käytännössä jäsenmaiden yhteisten kyberharjoitusten avulla.

Kokouksen yhteydessä EU-jäsenvaltiot antoivat yleistasoisen ”*Warsaw Call on Cybersecurity Challenges*” julistuksen. Julistus sisältää listauksen ei-sitovia unionin tason toimia, joilla tulisi vahvistaa unionin kyberturvallisuutta muuttuvassa toimintaympäristössä. Toimet sisältävät muun muassa kannustuksen vahvistaa olemassa olevia kyberturvallisuuden rakenteita, hyödyntää riskiarviointeja, saattaa

kyberlainsäädäntöä kansallisesti voimaan sekä vähentää lainsäädännöstä tulevaa hallinnollista taakkaa.

Suomen edustajat
Liikenne- ja viestintäministeri Lulu Ranne
Yksikönjohtaja Timo Kievari
Suunnittelija Petri Lepistö