Lepistö Petri 25.2.2025

Viite
Napsauta tähän ja kirjoita viite.

EU; Epävirallinen televiestintäministerikokous 4.-5.3.2025

EU:n televiestintäministerit kokoontuvat epävirallliseen ministerikokoukseen 4.-5.3.2025 Varsovassa. Suomea kokouksessa edustaa liikenne- ja viestintäministeri Lulu Ranne.

Televiestintäministerien epävirallisen kokouksen aiheena on kyberturvallisuus. Puheenjohtajan jakaman ennakkotiedon mukaan ministerit käyvät kolme keskustelua. Ensimmäisessä sessiossa ministerit keskustelevat EU:n yhteistoiminnasta ja reagoinnista kyberhäiriötilanteisiin. Työlounaan aiheena on siviili-sotilasyhteistyö kyberturvallisuudessa. Kolmannen keskustelun aiheena on investoinnit kyberturvallisuuteen.

Puheenjohtajamaa Puola on myös kyberturvallisuustematiikkaan liittyen esittänyt jäsenmaiden yhteisdeklaraation ”*Warsaw Call on Cybersecurity Challenges*” antamista epävirallisen ministerikokouksen yhteydessä.

Kyseessä on epävirallinen ministerikokous, jossa ei tehdä päätöksiä.

Asialista:

Keskustelu: EU:n yhteistoiminta ja reagointi kyberhäiriötilanteisiin (kyberblueprint päivitys) s.3

Keskustelu: Siviili-sotilasyhteistyö kyberturvallisuudessa s.3

Keskustelu: Investoinnit kyberturvallisuuteen s.3

Liikenne- ja viestintäministeriö Perusmuistio EU/199/2025-LVM-2

Hokkanen Emma, Lepistö Petri 25.2.2025

EU; Epävirallinen teleministerikokous (kyberturvallisuus) 4.-5.3.2025

Kokous
Epävirallinen EU-televiestintäministerikokous 4.-5.3.2025

Eduskuntatunnus

Käsittelyvaihe ja jatkokäsittelyn aikataulu

EU:n televiestintäministerit kokoontuvat epäviralliseen ministerikokoukseen Varsovaan 4.–5.3. puheenjohtajavaltio Puolan kutsusta. Kokous keskittyy kyberturvallisuuden kysymyksiin.

Kyseessä on epävirallinen ministerikokous, jossa ei tehdä päätöksiä.

Suomen kanta

Suomi painottaa yhtenäisen lähestymistavan, tiedonvaihdon ja yhteisen tilannekuvan sekä kriisivasteen tärkeyttä Euroopalle kyberturvallisuushaasteisiin vastaamiseksi. Suomi katsoo, että on Suomen edun mukaista vahvistaa kyberturvallisuutta myös EU:n yhteisillä toimilla, ja hakea ja hyödyntää kansallisten ja unionin tason toimien välisiä synergioita. Suomi katsoo, että uusien tilannekuva- ja tiedonvaihtotoimintojen perustamisessa tulee välttää päällekkäisyyksiä jo olemassa olevien toimintojen kanssa. (U 20/2023)

Suomen näkemyksen mukaan monimutkaiset ja rajat ylittävät kriisit edellyttävät yhä enemmän EU-tason varautumista, mukaan lukien yhteisiä kapasiteetteja ja suorituskykyjä. EU-tason yhteisten kapasiteettien kehittäminen tulee olla strategista ja pitkäjänteistä ja Suomi tukee tätä työtä. (E 32/2024)

Kehitettävien kyberkykyjen on vastattava Euroopan muuttuneeseen turvallisuus- ja toimintaympäristöön. On tärkeää hyödyntää siviili-sotilas-yhteistyön synergiat jäsenmaiden kyberpuolustuksen ja suorituskykyjen kehittämiseen. Suomi kannattaa vahvasti yhteistyön ja koordinaation tiivistämissä Naton kanssa kyberpuolustuksessa muun muassa

koulutuksessa, harjoituksissa sekä tilannekuvan jakamisessa mukaan lukien attribuutio. (E 175/2022)

Suomi pitää tärkeänä EU-rahoitusohjelmien uudistamista vastaamaan paremmin EU:n tulevia haasteita. Suomi katsoo, että varoja tulisi kohdentaa nykyistä vahvemmin valittujen strategisten prioriteettien mukaisesti. Suomi katsoo, että puolustuksen (ml. sotilaallinen liikkuvuus), kriisivarautumisen ja rajaturvallisuuden rahoituksen osuutta tulee kasvattaa huomattavasti nykyisestä suhteellisesti vähäisestä määrästä. (E 31/2024)

Pääasiallinen sisältö

Keskustelussa tulevat olemaan EU:n yhteistoiminta ja reagointi kyberhäiriötilanteisiin koordinoidusta reagoinnista laajamittaisiin kyberturvallisuuspoikkeamiin ja -kriiseihin annetun komission suosituksen ((EU) 2017/1584) (kyberblueprint) päivittämisen avulla, siviili-sotilasyhteistyö kyberturvallisuudessa sekä investoinnit kyberturvallisuuteen.

Kyberturvallisuuden lainsäädäntökehikkoa uudistettiin kattavasti edellisen komission kaudella ja jäsenmaat ml. puheenjohtajamaa Puola ovat painottaneet uuden lainsäädännön toimeenpanon tärkeyttä uuden sääntelyn sijaan.

Puheenjohtajamaa Puola on myös kyberturvallisuustematiikkaan liittyen esittänyt jäsenmaiden yhteisdeklaraation ”*Warsaw Call on Cybersecurity Challenges*” antamista epävirallisen ministerikokouksen yhteydessä.

Kyberblueprintin päivittäminen

Puolan puheenjohtajakauden prioriteettina kyberturvallisuudessa on päivittää EU:n kyberblueprint. Päivitetyssä kyberblueprintissä on tarkoitus määritellä EU:n toimintatapoja, vastetta, yhteistoimintaa ja eri instituutioiden työnjakoa rajat ylittävissä kyberhäiriötilanteissa nykyisen uhka- ja toimintaympäristön puitteissa.

Komissio antoi alkuperäisen kyberblueprintin vuonna 2017 komission suosituksena. Kyberblueprintissa vahvistettiin kriisinhallintakehys, yksilöitiin keskeiset sidosryhmät ja ehdotettiin kolmiportaista rakennetta (tekninen, operatiivinen ja poliittinen) noudattaen samalla suhteellisuus -, toissijaisuus -, täydentävyys - ja luottamuksellisuusperiaatteita. Suositus on monilta osin vanhentunut uuden kyberlainsäädännön ja toimintaympäristön muutoksen myötä. Alustavaa keskustelua tulevan päivitetyn kyberblueprintin sisällöstä on käyty neuvoston horisontaalisessa kybertyöryhmässä sekä teknisen tason asiantuntijaryhmissä. Jäsenmaiden ensisijainen toive on ollut saada selkeä, käytännönläheinen ja tiivis suositus, jossa määritellään eri toimintojen vastuut, roolit ja yhteistoiminta häiriötilanteissa.

Osana kyberblueprintin valmistelua, puheenjohtaja on halukas keskustelemaan jäsenmaiden välisen luottamuksen vahvistamisesta ja eri toimintojen yhteistoiminnasta kyberkriisienhallinnassa. Puheenjohtajan erityisenä tavoitteena on keskustella siitä, miten kyberkriisivaste ja muut kriisivasteet toimivat yhteen tilanteissa, joissa kyberturvallisuuspoikkeamalla on suora vaikutus johonkin muuhun toimintoon kuin tietojenkäsittelyyn, kuten esimerkiksi sähkönjakeluun tai terveydenhuoltoon. Lisäksi puheenjohtaja pyrkii tunnistamaan yksinkertaisia ja helposti toteutettavia toimia, joilla tiedonvaihtoa, tilannekuvaa ja koordinaatiota voidaan kehittää.

Siviili-sotilasyhteistyö kyberturvallisuudessa

Puheenjohtaja esittää keskustelua tavoista, joilla voidaan vahvistaa siviili-sotilasyhteistyötä muun muassa tiedonvaihdossa kyberuhkiin vastaamiseksi nykyjärjestelyjen

puitteissa, tunnistaa esteitä siviili-sotilasyhteistyölle ja vastata niihin, sekä yhteistyömahdollisuuksista Naton kanssa.

Vuonna 2022 annetussa EU:n kyberpuolustuspolitiikkaa koskevassa yhteisessä tiedonannossa todettiin, että sotilas - ja siviilikyberyhteisöjen välinen yhteistyö on perusta paremmalle yhteiselle kybertilannetietoisuudelle. EU:n kyberturvallisuusstrategiassa puolestaan todetaan, että kyberturvallisuus ja kyberpuolustus on edelleen integroitava osaksi laajempaa turvallisuus- ja puolustusagendaa. Niinistön raportissa todetaan, että erityistä huomiota olisi kiinnitettävä puutteiden tai päällekkäisyyksien tunnistamiseen operatiivisella tasolla nopeiden, tehokkaiden ja läpileikkaavien EU:n toimien varmistamiseksi. Raportissa suositeltiin siviili-sotilaskoordinaatiokehysten vahvistamista ja yhteistä suunnittelua, jotta voidaan varmistaa tehokas siviili-sotilastoiminta erilaisiin tahallisiin uhkiin sekä EU:ssa että sen ulkopuolella.

Investoinnit kyberturvallisuuteen

Kuluvalla rahoituskehyskaudella pääasiallinen rahoitusmekanismi kyberturvallisuuden vahvistamiseksi ja kyberturvallisuuden teollisuuden edistämiseksi on ollut Digitaalinen Eurooppa-ohjelma. Ohjelmasta on rahoitettu kyberturvallisuutta tähän mennessä noin 600 miljoonalla eurolla, josta Suomen saanti on tähän mennessä ollut 10,2 miljoonaa euroa. Koko rahoituskehyskaudella kyberturvallisuuden osuus Digitaalinen Eurooppa-ohjelmassa on noin 1,37 miljardia euroa.

Euroopan komission on määrä julkaista ehdotus seuraavasta tutkimuksen- ja innovoinnin puiteohjelmasta vuoden 2025 aikana. Ehdotuksen sisältöön vaikuttavat Horisontti Euroopan väliarvioinnin tulokset sekä vuoden 2024 aikana julkaistut eri asiantuntijaryhmien tuottamat selvitykset, kuten Niinistön, Draghin ja Lettan raportit. Komission tammikuussa julkaistussa kilpailukykykompassissa lisäksi todetaan, että Euroopan on oltava eturintamassa innovaatioissa niillä teknologia-aloilla, joilla on merkitystä teknologisen riippumattomuuden ja kilpailukyvyn lisäämiseksi. Lisäksi kilpailukykykompassissa korostetaan, että Euroopan on otettava huomioon digitaalisen tai fyysisen kriittisen infrastruktuurin turvallisuuteen liittyvät riskit kaikissa vaiheissa.

Investointien osalta odotetaan puheenjohtajalta lisätietoja keskusteluun.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

Kokouksessa ei tehdä päätöksiä.

Käsittely Euroopan parlamentissa

-

Kansallinen valmistelu

Viestintäjaosto (EU19), 20.2.2025
EU-ministerivaliokunta, 28.2.2025

Eduskuntakäsittely

Suuri valiokunta, 28.2.2025, kirjallinen menettely

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

-

Taloudelliset vaikutukset

-

Muut asian käsittelyyn vaikuttavat tekijät

-

Asiakirjat

Puheenjohtajan tausta-asiakirjat (osittain jaettu)

Laatijan ja muiden käsittelijöiden yhteystiedot

Erityisasiantuntija, Emma Hokkanen, liikenne- ja viestintäministeriö, +358295342106
Suunnittelija, Petri Lepistö, liikenne- ja viestintäministeriö, +358295342014

VAHVA-tunnus

EU/199/2025