Hallintovaliokunta
HaV@eduskunta.fi

Asiantuntijalausunto hallintovaliokunnalle valtioneuvoston selvityksestä: Suomen avaintavoitteet EU-vaalikaudelle 2024-2029 (E 58/2023 vp)

Hallintovaliokunta on pyytänyt Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselta kirjallista lausuntoa valtioneuvoston selvityksestä koskien Suomen avaintavoitteita EU-vaalikaudelle 2024-2029 (E 58/2023 vp). Liikenne- ja viestintäviraston Kyberturvallisuuskeskus kiittää mahdollisuudesta lausua asiassa. Liikenne- ja viestintävirasto yhtyy valtioneuvoston kannassa esitettyihin Suomen avaintavoitteisiin sekä pääprioriteetteihin. Virasto korostaa valtioneuvoston kannassa kuvatulla tavalla aloitteellisen, rakentavan ja ennakoivan lähestymistavan tärkeyttä Suomen tavoitteiden edistämiseksi seuraavalla EU-vaalikaudella. Liikenne- ja viestintävirasto lausuu kyberturvallisuuden osalta seuraavasti:

Kyberturvallisuusuhkat, -häiriöt ja -hyökkäykset tulevat nykyään aiempaa konkreettisimmin esille - samalla tavoin kuin fyysisessä maailmassa kohtaamamme turvallisuusuhkat ja muut häiriöt. Esimerkiksi huijaukset, palvelunestohyökkäykset, haittaohjelmat ja kiristyshyökkäykset organisaatioiden ICT-ympäristöihin sekä tietojenkalastelu vaikuttavat suomalaisten ja Suomessa toimivien organisaatioiden arkeen. Yhteiskunnan eri palveluiden digitalisoituessa kyberturvallisuusuhat eivät ole enää erillisen virtuaalimaailman vitsaus, vaan valtioiden, organisaatioiden ja ihmisten jokapäiväiseen elämään vaikuttava uhka. Monesti nämä uhkakuvat voivat kohdistua myös yhteiskunnan toiminnan kannalta kriittisiin toimintoihin. Liikenne- ja viestintävirasto muistuttaa, että kyberrikollisten ja muiden kybertoimijoiden kyvykkyydet ja erilaiset kyberturvallisuutta koskevat häiriöt sekä hyökkäykset kehittyvät alati kehittyvän teknologian ohella. Suomalaisella ja eurooppalaisella yhteiskunnalla tulee olla valmius vastata näihin uhkiin.

Turvallisuusympäristömme on pysyvästi muuttunut eikä kyberriskejä voida enää arvioida irrallaan muista turvallisuusriskeistä. Uusien riskien tunnistaminen ja niihin vastaaminen edellyttää kansallista ja kansainvälistä poikkihallinnollista seurantaa, analyysiä ja varautumista. Kyberturvallisuuden uhkataso on pysyvästi muuttunut ja tähän vastaaminen edellyttää uusia ja tehokkaampia toimia sekä yhteistyötä koko Euroopassa. Turvallisuuden kokonaistilannekuvalla on kasvanut tarve yritysten ja viranomaisten toiminnassa sekä valtiojohdossa. Kansainvälisellä ja kansallisella tiedonvaihdolla on keskeinen osa siinä, miten lyhyen ja pitkän aikavälin kyberriskeihin tulee varautua. Tässä tiedonvaihdossa Kyberturvallisuuskeskuksella on pitkät perinteet ja Euroopan unioni on yksi keskeisimmistä verkostoista mainitun tiedonvaihdon viitekehyksenä. Euroopan lisäksi kyberturvallisuudessa korostuu tiivis yhteistyö niin Naton piirissä kuin luotettujen kumppanimaiden kanssa.

Liikenne- ja viestintävirasto pitää tärkeänä, että kyberturvallisuutta vahvistetaan laajasti myös Euroopan unionin tasolla tulevaisuudessa. Kyberturvallisuus on keskeinen osa unionin ja Suomen kokonaisturvallisuutta ja kyberturvallisuuden merkitys on korostunut entisestään muuttuneessa turvallisuusympäristössä. Kyberturvallisuuden vahvistaminen edellyttää myös lainsäädännön tarkastelua teknologioiden kehittyessä ja uhkaympäristön muuttuessa. Liikenne- ja viestintävirasto pitää tärkeänä, että kyberturvallisuus on sisäänrakennettua digitalisaation eri kehitysvaiheissa kuin myös murrosteknologioiden kehityksessä.

On syytä varmistaa, että myös EU-tason sääntely mahdollistaa riittävän yhteistyön ja tiedonvaihdon mahdollisuudet niin rajat ylittävästi kuin kansallisesti. Viranomaisyhteistyön ja sitä tukevan sääntelyn kehittäminen on tärkeää koko EU:n kyberturvallisuuden kehittämiseksi ja varmistamiseksi. Kyberloukkausten selvittäminen ja ennaltaehkäiseminen edellyttävät monissa tapauksissa vastavuoroista tietojen vaihtoa, tiivistä yhteistyötä ja toimia usealta toimivaltaiselta viranomaiselta. Toisaalta on syytä pitää mielessä, että myös tulevaisuudessa on tärkeää löytää tasapaino yhtäältä viranomaisten tiedonjaon mahdollistamisen ja toisaalta viestinnän luottamuksellisuuteen tai salassapitoperusteisiin tehtävien rajoitusten välillä.

Liikenne- ja viestintävirasto korostaa, että EU:n tasolla on annettu viime vuosina merkittävä määrä kyberturvallisuutta koskevia lainsäädäntöehdotuksia. Esityksillä on ollut tärkeä vaikutus muun muassa kriittisen infrastruktuurin turvallisuuden ja tuotteiden sekä palveluiden kyberturvallisuuden kehittämisessä. Liikenne- ja viestintävirasto haluaa kuitenkin muistuttaa, että uusien ehdotusten laatimisen ja käsittelyn yhteydessä on ensiarvoisen tärkeää pyrkiä välttämään päällekkäisiä toimia ja toimenpiteitä. Vahvana lähtökohtana tulisi olla, että uusien ehdotusten taustalla on yhteisesti tunnistettuja tarpeita ja kehityskohteita sekä tarvittavaa vaikutustenarviointia. On syytä huomioida, että kyberturvallisuuden edistäminen ei edellytä kaikissa tapauksissa yksinomaan velvoittavaa sääntelyä. Esimerkiksi kyberturvallisuutta koskevassa yhteistyössä on tyypillistä verkostomainen työskentelytapa, joka perustuu monesti osallistujien keskinäiseen luottamukseen ja toiminnan vapaaehtoisuuteen.

Kyberympäristön muutoksista huolimatta Suomen panostukset kyberturvallisuuteen ovat viimeisen vuosikymmenen ajan jääneet jälkeen uhkien kehittymisestä. Panostukset kyberosaamisen kehittämiseen niin Suomessa kuin EU:ssa yleisemminkin ovat olleet puutteellisia. Liikenne- ja viestintävirasto pitää välttämättömänä, että toimintaympäristön muutoksesta sekä kasvavasta sääntelystä johtuva tehtävämäärä Kyberturvallisuuskeskuksen ja muiden suomalaisten viranomaisten toiminnassa huomioidaan pysyvästi jatkossa. Vallitsevassa maailmantilanteessa Kyberturvallisuuskeskuksen apua tai palveluita tarvitsevia kansalaisia, viranomaisia ja yhteiskunnan kriittisten toimialojen toimijoita on joka vuosi entistä enemmän. Mikäli jäämme jälkeen Suomen kyberturvallisuuden perustan rakentamisessa, tulevat tulevaisuuden kustannukset kyberturvallisuuden toimenpiteiden laiminlyönnistä olemaan moninkertaisesti suhteessa nyt tarvittaviin panostuksiin. Samanlaisia panostuksia ja niiden lisäämistä tarvitaan myös koko Euroopan unionissa tulevalle vaalikaudelle 2024-2029.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus