Punkt i protokollet PR 41/2025 rd

Plenum

Onsdag 23.4.2025 kl. 14.00—17.51

7. Regeringens proposition till riksdagen med förslag till lagar om ändring av cybersäkerhetslagen och 3 § i lagen om informationshantering inom den offentliga förvaltningen

Regeringens proposition RP 27/2025 rd

Remissdebatt

Förste vice talman Paula Risikko: Ärende 7 på dagordningen presenteras för remissdebatt. Talmanskonferensen föreslår att ärendet remitteras till kommunikationsutskottet.

För debatten reserveras i detta skede högst 30 minuter. Om vi inte inom denna tid hinner gå igenom talarlistan avbryts behandlingen av ärendet och fortsätter efter de övriga ärendena på dagordningen. — Föredragande också i detta ärende är minister Ranne. Varsågod.

Debatt

15.42 **Liikenne- ja viestintäministeri Lulu Ranne** (esittelypuheenvuoro): Arvoisa puhemies! Meillä on täällä käsittelyssä hallituksen esitys eduskunnalle laeiksi kyberturvallisuuslain ja julkisen hallinnon tiedonhallinnasta annetun lain 3 §:n muuttamisesta. Tieto- ja viestintäteknologia on keskeinen osa nykyaikaista yhteiskuntaa ja sen kriittistä infrastruktuuria. Yhä useammat palvelut ja toiminnot ovat kasvavassa määrin riippuvaisia viestintäverkkojen ja tietojärjestelmien luotettavasta toiminnasta. Viestintäverkkojen ja tietojärjestelmien kyberturvallisuuteen voi kohdistua monenlaisia riskejä. Yhteiskunnan kokonaisturvallisuuden kannalta on tärkeää kasvattaa kyberturvallisuuden tasoa viestintäverkoissa ja kaikissa tietojärjestelmissä. Erityisen tärkeää se on silloin kun kysymys on yhteiskunnan toiminnan kannalta kriittisimmistä palveluista ja niiden toiminnan jatkuvuudesta.

Tämän esityksen tarkoituksena on täydentää Euroopan unionin kyberturvallisuusdirektiivin eli NIS kakkosen sekä kriittisten toimijoiden häiriönsietokyvystä annetun CER-direktiivin täytäntöönpanoa Suomessa. Hallituksen esityksen ja sen taustalla olevien direktiivien tavoitteena on vahvistaa kyberturvallisuuden ja häiriönsietokyvyn tasoa yhteiskunnan toiminnan kannalta kriittisimmissä organisaatioissa. Muun ohella tavoitteena on vähentää kyberhäiriöiden määrää sekä välttää kyberturvallisuuteen liittyvien poikkeamien aiheuttamia vakavia häiriöitä yhteiskunnan toiminnan kannalta kriittisimmissä palveluissa.

Esityksellä ehdotetaan kyberturvallisuuslakiin ja julkisen hallinnon tiedonhallinnasta annettuun lakiin niiden soveltamisalaa koskevia täydennyksiä sekä eräitä teknisiä muutoksia. Esityksen tavoitteena on toteuttaa lainsäädäntömuutokset, jotka ovat tarpeen kyberturvallisuuslain ja tiedonhallintalain kyberturvallisuuteen liittyvien velvoitteiden soveltamiseksi tulevaisuudessa myös niihin toimijoihin, jotka määritetään kriittisiksi toimijoiksi yhteiskunnan kriittisen infran suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla.

Nyt ehdotettava hallituksen esitys liittyy eduskunnassa käsiteltävänä olevaan hallituksen esitykseen laiksi yhteiskunnan kriittisen infran suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi. Esitysten välinen yhteys olisi tarpeen ottaa huomioon myös hallituksen esityksen 205/24 käsittelyn yhteydessä.

Ehdotukset vastaisivat vähimmäistasoa siitä, mitä NIS 2 -direktiivi ja CER-direktiivi edellyttävät kyberturvallisuutta koskevien velvoitteiden ja niiden valvonnan tasosta kriittisille toimijoille.

Hallituksen esitys on valmisteltu virkatyönä liikenne- ja viestintäministeriössä yhteistyössä sisäministeriön ja valtiovarainministeriön kanssa. Pidämme erittäin tärkeänä, että kyberturvallisuutta, tietoturvaa ja tietosuojaa vahvistetaan jatkossakin yhteiskunnan toiminnan kannalta kriittisillä toimialoilla yhteistyössä eri toimijoiden välillä. — Kiitos.

Ensimmäinen varapuhemies Paula Risikko: Kiitoksia. — Edustaja Hänninen.

15.45 **Juha Hänninen kok:** Kiitos, arvoisa rouva puhemies! Kiitän ministeri Rannetta erinomaisesta esittelystä ja työstä. Kiitos.

Turvallisuus ei ole vain fyysisiä rajoja tai näkyviä uhkia. Yhä useammin se on sitä, mitä tapahtuu tietoverkoissa, järjestelmissä ja palveluissa, joita arjessamme käytämme — tapahtumia, joihin kiinnitämme huomiomme vasta kun järjestelmämme ei toimi. Ja on totta, että jos nämä kaatuvat, kaatuu moni muukin asia ympärillämme.

Arvoisa rouva puhemies! Tänään käsiteltävä lakiesitys tähtää siihen, että yhteiskunnan toiminnan kannalta keskeiset palvelut pysyvät pystyssä myös poikkeustilanteissa. Tämä tarkoittaa esimerkiksi liikenteen, terveydenhuollon, julkisen liikenteen ja lääkkeiden jakelun kaltaisia toimintoja. Näissä palveluissa ei ole varaa katkoksiin. Esityksen mukaan tulevaisuudessa kaikki toimijat, jotka määritellään yhteiskunnalle tärkeiksi, velvoitetaan huolehtimaan paremmin järjestelmiensä kestävyydestä. Tämä tarkoittaa ennakointia, valvontaa ja toimintasuunnitelmia häiriöiden varalle.

Arvoisa rouva puhemies! Maailmantilanne on epävakaa. Häiriöitä syntyy, ja niitä myös luodaan tarkoituksella. Siksi meidän on nyt oltava askel edellä. Tähän asti osa tärkeistä palveluista on jäänyt velvoitteiden ulkopuolelle, erityisesti pienemmät yritykset, tietyt liikenteen toimijat ja esimerkiksi lääkealan jakelutahot. Tällä esityksellä tuo puute nyt korjataan. Turvallisuus on meidän jokaisen tehtävä. Kyse ei ole hallinnon paisuttamisesta. Kyse on siitä, että myös pienempi toimija, jolla on suuri merkitys yhteiskunnan toimivuudelle, osaa varautua häiriöihin. Näin kansalaisten luottamus palveluihin säilyy silloin kun normaali ei toimi. On tärkeää, että viranomaiset tekevät yhteistyötä, jakavat tietoa ja tukevat toimijoita ennakkoon. Näin vältetään yllättävät katkokset ja suojataan niitä, joiden arki on riippuvainen toimivista palveluista.

Arvoisa rouva puhemies! Tässä esityksessä kiteytyy yksi asia: Varautuminen on tämän päivän vastuullisuutta. Se ei aina näy ulospäin, mutta sen vaikutus tuntuu heti, jos sitä ei ole tehty. Tämä on tärkeä askel vakaamman ja luotettavamman ja turvallisemman yhteiskunnan puolesta. — Kiitoksia, arvoisa rouva puhemies.

Ensimmäinen varapuhemies Paula Risikko: Kiitoksia. — Edustaja Mikkonen, Anna-Kristiina.

15.49 **Anna-Kristiina Mikkonen sd:** Arvoisa puhemies! Tällä hallituksen esityksellä saatettaisiin kyberturvallisuuslain sekä julkisen hallinnon tiedonhallinnasta annetun lain soveltamisalaa koskemaan sellaisia yhteisöjä, jotka määritetään yhteiskunnan toiminnan kannalta kriittisiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla.

Tällä esityksellä täydennettäisiin kriittisten toimijoiden häiriönsietokykyä koskevan Euroopan parlamentin ja neuvoston direktiivin sekä kyberturvallisuutta koskevan Euroopan parlamentin ja neuvoston direktiivin kansallista täytäntöönpanoa. Tieto- ja viestintäteknologia sekä niihin liittyvät palvelut ovat keskeinen osa nykyaikaista yhteiskuntaa ja sen kriittistä infraa. Kehittyneet tieto- ja viestintäteknologiset ratkaisut mahdollistavat uusia innovaatioita, toimintatapoja ja palveluita yhteiskunnassa. Samaan aikaan yhä useammat palvelut ja toiminnot ovat kasvavassa määrin riippuvaisia viestintäverkkojen ja tietojärjestelmien luotettavasta toiminnasta. Viestintäverkkojen ja tietojärjestelmien kyberturvallisuuteen kohdistuu monenlaisia riskejä, jotka toteutuessaan aiheuttavat häiriöitä ja haittoja erilaisten syy-yhteyksien seurauksena. Häiriön tai haitan toteutuminen voi olla seurausta tahattomasta vahingosta tai tahallisesta oikeudettomasta teosta, jonka taustalla olevat motiivit vaihtelevat.

Tämä lakiesitys on tarkoitettu tulemaan voimaan samanaikaisesti yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain kanssa.

Suomi on maana ja tietoyhteiskuntana riippuvainen viestintäverkkojen ja tietojärjestelmien toiminnasta ja näin ollen myös haavoittuvainen niihin kohdistuville häiriöille. Yhteiskunnan kokonaisturvallisuuden kannalta on tärkeää kasvattaa kyberturvallisuuden tasoa niin viestintäverkoissa kuin tietojärjestelmissä.

Ensimmäinen varapuhemies Paula Risikko: Kiitoksia. — Edustaja Strandman.

15.51 **Jaana Strandman ps:** Arvoisa rouva puhemies! Kunnioitettu ministeri! Esityksessä ehdotetaan muutettavaksi kyberturvallisuuslakia ja julkisen hallinnon tiedonhallinnasta annettua lakia. Esityksellä saatettaisiin kyberturvallisuuslain sekä julkisen hallinnon tiedonhallinnasta annetun lain soveltamisala koskemaan sellaisia yhteisöjä, jotka määritetään yhteiskunnan toiminnan kannalta elintärkeiksi kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain nojalla.

Esityksellä täydennettäisiin kriittisten toimijoiden häiriönsietokykyä koskevan EU-direktiivin kansallista täytäntöönpanoa. Hallitusohjelman mukaan kyberturvallisuutta ja sitä koskevaa yhteistyötä viranomaisten ja elinkeinoelämän välillä vahvistetaan, hallitus parantaa tietoturvaa kriittisillä toimialoilla ja EU-lainsäädännön toimeenpanon yhteydessä vältetään kansallista lisäsääntelyä. Lait on tarkoitettu tulemaan voimaan samanaikaisesti yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ehdotetun lain kanssa.

Arvoisa rouva puhemies! Kyberturvallisuus on kansallista turvallisuutta. Geopoliittinen tilanne erityisesti itäisen naapurimme suhteen on merkki siitä, että turvallisuudesta ei voi joustaa. Kyberturvallisuuden vahvistaminen on osa kriisinkestävyyttä ja itsenäisyyttä sekä mahdollistaa Suomen itsemääräämisoikeuden sekä itsenäisyyden. Perussuomalaiset ovat jo pitkään painottaneet kyberpuolustuksen merkitystä puolustuksessa. Kyberhyökkäykset voivat pahimmillaan lamaannuttaa koko yhteiskunnan ja sen kriittiset toiminnot. Tieto-,

energia- ja huoltovarmuussektorit ylipäätään ovat merkittävässä asemassa. Kyberhyökkäyksen lopputulema voi olla aivan yhtä vahingollinen kuin perinteisenkin sodankäynnin.

Esityksellä on vähäinen vaikutus kyberturvallisuuslakia valvovien viranomaisten tehtävämäärään. Kustannukset julkiselle ovat arvioiden mukaan vähäiset. Yritysten osalta ei ole kustannuksia, paitsi niille yrityksille ja yhteisöille, joita esitys koskee. Vaikutukset yritysten osalta riippuvat pitkälti siitä, kuuluvatko ne jo valmiiksi kyberturvallisuusvelvoitteiden soveltamisalaan. Niille yrityksille, jotka tulevat kriittiseksi määrittämisen takia uusina organisaatioina kyberturvallisuuden soveltamisalaan, olisi esityksellä taloudellisia vaikutuksia.

Esityksellä olisi myönteisiä vaikutuksia tietoyhteiskunnan kehitykseen, sillä se edistäisi tietoturvallisuuden palvelujen ja käytänteiden käyttöönottoa ja siten loisi kysyntää tällaisille palveluille sekä kyberturvallisuuden ammattilaisille. Kyberturvallisuustason parantuminen vähentäisi palvelujen käytössä esiintyviä häiriöitä ja edistäisi yleistä luottamusta digitaalisiin palveluihin. Esityksellä arvioidaan olevan yhteiskunnan häiriöttömän toiminnan edistämisen kautta myönteisiä vaikutuksia kansalaisten turvallisuudelle. Esitys edistää yhteiskunnan toiminnan kannalta kriittisten toimijoiden kykyä sietää kyberhäiriöitä, millä parannetaan kansalaisten turvallisuutta erityisesti silloin, kun toimialassa tai palvelussa kyse on kansalaisten turvallisuuteen vaikuttavista, yhteiskunnan toiminnan kannalta kriittiseen infrastruktuuriin liittyvistä toiminnoista.

Kiitän ministeri Rannetta tämän asian tuomisesta tänne saliin. — Kiitos.

Ensimmäinen varapuhemies Paula Risikko: Kiitoksia. — Edustaja Seppänen.

15.55 **Sara Seppänen ps:** Arvoisa rouva puhemies! Kyberturvallisuus ei ole pelkkä tekninen kysymys. Kyberhyökkäys voi pahimmillaan olla yhtä tuhoisa kuin aseellinen hyökkäys, jos se lamauttaa energiajakelun, tietoverkot tai muun kriittisen infrastruktuurin.

Hallituksen esityksellä kyberturvallisuuslain ja tiedonhallintalain muuttamisesta vastataan muuttuneeseen turvallisuusympäristöön. Esityksessä ehdotetaan muutettavaksi kyberturvallisuuslakia ja julkisen hallinnon tiedonhallinnasta annettua lakia siten, että niiden soveltamisala ulotettaisiin koskemaan myös sellaisia yhteisöjä, jotka on määritelty osaksi yhteiskunnan kriittistä infrastruktuuria. Me perussuomalaiset tuemme tätä esitystä, koska se vahvistaa Suomen kriisinkestävyyttä, itsenäisyyttä ja suojaa meitä ulkoisilta vaikuttamisyrityksiltä.

Geopoliittinen tilanne on epävakaa, ja kyberuhat ovat yhä monimuotoisempia. Vahva kyberturvallisuus suojaa yhteiskuntaa, ei vain viranomaisten järjestelmiä vaan myös tavallisten suomalaisten arkea. On tärkeää, että viranomaisilla on ajantasaiset työkalut suojautua kyber- ja hybridivaikuttamiselta. Lainsäädännön tulee tukea viranomaisten ja muiden toimijoiden kykyä torjua kyberuhkia ilman tarpeetonta byrokratiaa.

Perussuomalaiset painottavat, että Suomen tulee panostaa entistä vahvemmin kyberpuolustukseen. Olemme nyt osa Natoa, se antaa meille mahdollisuuden kehittää osaamistamme ja varautumistamme entistä korkeammalle tasolle. Meidän on varmistettava, että viranomaisprosessit tukevat nopeaa ja tehokasta reagointia hybridioperaatioihin ja kyberhyökkäyksiin.

Kannatan tätä kansalaisten tietoturvan, Suomen itsenäisyyden ja yhteiskunnan toimintakyvyn turvaamista ja sitä parantavia lakeja. Tämä lakiesitys ansaitsee kyllä vahvan tuen tässä salissa.

Ensimmäinen varapuhemies Paula Risikko: Kiitoksia. — Edustaja Mäkinen.

15.57 **Riitta Mäkinen sd:** Arvoisa rouva puhemies! Nyt käsittelyssä olevassa hallituksen esityksessä ehdotetaan muutettavaksi kyberturvallisuuslakia ja julkisen hallinnon tiedonhallinnasta annettua lakia, jonka kautta on tarkoitus toimeenpanna kansallisella tasolla käytäntöön EU:n kyberturvallisuusdirektiivien mukaista sääntelyä, niin kutsuttua CER-direktiiviä ja NIS 2 -direktiiviä. Niiden tarkoituksena on vahvistaa EU:n yhteistä ja sen jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta keskeisillä toimialoilla näiden toimijoiden häiriönsietokykyä vahvistamalla. Molemmat direktiivit ovat EU-lainsäädännön vähimmäissääntelyä, mikä tarkoittaa käytännössä, että kansallinen liikkumavara koskee lähinnä toimintaa valvovien viranomaisten nimeämistä ja seurausten määrittelyä.

Arvoisa puhemies! Hallituksen esitys tarkoittaa suomeksi, että nyt säädettäisiin lailla yhteiskunnan kriittiseksi katsomien yritysten ja organisaatioiden kuulumisesta kyberturvallisuuslain mukaisten vaatimusten alaisuuteen kyberturvallisuudesta huolehtimisen, valvonnan ja raportoinnin osalta. Samalla viranomaisille annettaisiin mahdollisuus ohjata ja asettaa myös seurauksia mahdollisten laiminlyöntien johdosta.

Tätä lakia on odotettu jo hyvä tovi. Kaiken kaikkiaan tällaista lainsäädäntöä voidaan pitää kannatettavana, jollei jopa välttämättömänä, sillä kyberturvallisuus on yksi keskeinen yhteiskunnallisen turvallisuuden ja vakauden pilari. Ympäröivä maailma ja toimintaympäristö on muuttunut entistä epävakaammaksi, ja meidän on myös Suomessa tehtävä kaikki mahdollinen kyberturvallisuuden vahvistamiseksi myös niin sanotusti siviilitoimijoiden keskuudessa yhteiskunnan vahvasti läpileikaten. Esimerkiksi kyberrikollisuuden tai hybridivaikuttamisen yleistyminen ja osin arkipäiväistyminen edellyttävät koko yhteiskunnalta uudenlaisia toimia sen aiheuttamiin uhkiin ja haasteisiin vastaamiseksi.

Arvoisa puhemies! Haluan osaltani kiinnittää erityistä huomiota seuraaviin seikkoihin: Nyt käsillä olevan sääntelyn toimeenpano käytännössä riippuu pitkälle eri viranomaisten todellisesta kyvystä valvoa lainsäädännön piiriin kuuluvia toimijoita. Prosessien tulisi olla selkeitä ja kustannustehokkaita, eikä niiden tule vaikeuttaa yritysten ja organisaation varsinaista toimintaa. Esitän erityisen huolenaiheeni koskien kuitenkin näitä resursseja, koska olen vähän huolissani siitä, että samaan aikaan kun valvontaa harjoittavien viranomaisten ja viranomaisorganisaatioiden resursseja leikataan, niin uusia lisätehtäviä tullaan kuitenkin osoittamaan, ja valiokunnan kuulemisissakin on todettu, että tätä pidetään aika lailla kestämättömänä yhtälönä. Toivon tältä osin, että tähän asiakokonaisuuteen kiinnitetään sen ansaitsema huomio ja suhtaudutaan siihen sillä vakavuudella, jolla tulee, koska olen aivan vakuuttunut siitä, että läheskään kaikkea sitä, mitä kyberturvallisuuden edistämiseksi tässä yhteiskunnassa tulee tehdä, ei vielä ole tehty.

Puhemies Jussi Halla-aho: Kiitoksia. — Edustaja Harakka, olkaa hyvä.

16.00 **Timo Harakka sd:** Arvoisa puhemies! Suomalaisen yhteiskunnan turvallisuuden takaamisessa meillä on yksi kansainvälisestikin arvostettu, täysin ainutlaatuinen valtti. Se on niin sanottu PTR-yhteistyö, jossa poliisi, Tulli ja Raja ovat pystyneet aivan poikkeuksellisella tavalla yhteiseen tietojenvaihtoon, tilannekuvaan, johtojärjestelmien joustavaan siirtämiseen, jopa johtovastuiden siirtämiseen sekä yhteisten resurssien käyttöön tilanteen

niin vaatiessa, ja juuri tämän ansiosta tuo joulupäivänä pysäytetty Eagle S -laiva oli erinomainen esimerkki tästä aivan ainutlaatuisesta viranomaisyhteistyöstä.

Jo edellisellä hallituskaudella tavoitteena oli saada tämä samantapainen niin sanottu kyber-PTR voimaan myöskin digitaalisessa ympäristössä ennakoiden sitä, että digi- ja dataverkot ovat erityisen hyökkäyksen kohteena ja myöskin datasisällöt haavoittuvaisia, jolloin valtioneuvoston periaatepäätös jo kesältä 21, eli siis neljän vuoden takaa, tunnisti tietoturvan, tietosuojan parantamisen tarpeet näillä yhteiskunnan kriittisillä toimialoilla ja luetteli 37 toimenpidettä. Tämä eri viranomaisten tiivistetty yhteistyö ja tietojenvaihto tuotiin sitten eduskuntaan, jotta Kyberturvallisuuskeskus, poliisi ja Puolustusvoimat voisivat samaan tapaan kuin poliisi, Tulli ja Raja toimia joustavasti yhteistyössä tilanteen niin vaatiessa, mutta valitettavasti tämä esitys jäi tänne eduskunnan valiokuntiin ja raukesi.

Olisi ollut hyvä saada tämä niin sanottu kyber-PTR tai viranomaisten tiivistetty yhteistyö voimaan jo kansallisella lainsäädännöllä ennen kuin EU teki NIS 2- ja CER-lainsäädännöt, joita tässä nyt pannaan täytäntöön, koska meillä olisi varmasti ollut tässä hyvää kokemusta ja olisimme varmaan voineet myöskin Euroopan unionia auttaa siltä osin, että oltaisiin saatu varmuudella tarkoituksenmukaisimmat ja tehokkaimmat lainsäädännöt. Nyt tilanne on se, että pannaan toimeen useita kuukausia myöhässä tällaista yhteensovittamista CER-direktiivin ja NIS 2 -direktiivin osalta kansallisella tasolla. Tämä ei ole lainkaan yhtä kunnianhimoinen kuin tämä meidän kansallinen alkuperäinen suunnitelma oli, mutta totta kai on erittäin kannatettavaa, että viranomaisten joustava yhteistyö ja tietojenvaihto mahdollistuvat, ja myöskin se, että kriittisten toimialojen luettelo tässä laajenee asianmukaisesti.

Yhdyn edustaja Mäkisen huoleen siitä, että tyypilliseen EU-lainsäädäntötapaan esitetään paljon uusia velvoitteita ja vaatimuksia kansallisille viranomaisille ja sitten jää kansallisille toimijoille liikkumavaraksi ainoastaan myöntää käytännössä resurssit näille uusille tehtäville. Jo lausuntovaiheessa on esitetty huolta siitä, onko mahdollista, että varmasti nämä uudet tehtävät tulevat tiukoissa valtiontalouden raameissa sitten toteutetuiksi. Tämä on erittäin tärkeä kysymys. Ennen kaikkea Energiavirasto on esittänyt huolenaiheita — kun he odottavat, että heillä saattaa resurssit jopa vähetä — pystyvätkö he omalta osaltaan nämä vaatimukset täyttämään, ja tietenkin Kyberturvallisuuskeskus ylisummaan sekä Traficomin kaikki toiminnot ovat jo pitkään olleet kestokyvyn rajoilla, joten pyydän ministeriä vakuuttamaan meidät kaikki siitä, että kyberturvallisuuden edistäminen ei jää siitä kiinni, että nämä tärkeät toimijat eivät saa tarvitsemiaan resursseja, ja kuulisin mielelläni, minkälaisia lisäresursseja kyberturvallisuuteen olette esittänyt.

Puhemies Jussi Halla-aho: Kiitoksia. — Ja ministeri Ranne, viisi minuuttia, olkaa hyvä.

16.05 **Liikenne- ja viestintäministeri Lulu Ranne:** Arvoisa puhemies! Ensin totean, että Suomen kyberturvallisuusstrategiahan uudistettiin viime vuonna ja se saatiin varsin mallikkaana ulos sieltä. Tämän osalta voisi todeta myös sen, että Euroopassa on seurattu meidän kyberturvallisuuskehitystä hyvin tiiviisti ja me olemme myöskin vuorovaikuttaneet sinne suuntaan. Me olemme varsinainen mallioppilas tässä, vaikkakin resurssimme voisivat olla paremmat.

Meillä on tälläkin hetkellä Traficomin alaisuudessa Kyberturvallisuuskeskus, jota tullaan ihailemaan ympäri Eurooppaa, vähän laajemminkin. Meillä on liikenne- ja viestintäministeriössä kyberturvallisuusjohtaja, ja uusi apulaiskyberturvallisuusjohtajakin aloitti

juuri. Eli tarvitsemme tietenkin jatkuvaa kehittämistä kyberturvallisuuden sektorilla, ja voin todeta, että omalla hallinnonalallani, Traficomilla, ei ole ainakaan pienennetty resursseja, jotka ovat liittyneet tähän, ja toki haemme koko ajan mahdollisuuksia. Nytkin meillä on riihi tuolla vielä edelleen käynnissä.

Ehkä muutama sana vielä turvallisuusviranomaisten välisestä yhteistyöstä. Eli voi hyvinkin todeta, että liikenne- ja viestintäministeriö on varsinainen turvallisuusministeriö, ja me olemme tiivistäneet yhteistyötämme niin poliisin, Tullin kuin Rajan ja esimerkiksi supon kanssa tämän hallituskauden ajan. Meillä on myöskin ihan uusia yhteistyön toimintatapoja, ja yhteys on varsin tiivistä.

Jaamme kyllä huolen siitä, että maailma on muuttunut. Meillä on ”cyber as a crime”, meillä on todella vaarallisia liikkeitä, ja tietenkin Suomen täytyy tässä koko verkkoturvallisuusasiassa pyrkiä parempaan. Sisäministeriön kanssa teemme myöskin erittäin tiivistä yhteistyötä. — Kiitoksia.

Puhemies Jussi Halla-aho: Kiitoksia. — Edustaja Harakka, olkaa hyvä.

16.07 **Timo Harakka sd:** Arvoisa puhemies! Kiitos ministerille vastauksesta ja näistä vakuutuksista siitä, että huolehditaan asianmukaisista resursseista näille viranomaistoimijoille.

Toinen asia kokonaan on se, että se heikoin lenkki kyberturvallisuudessa saattaa kuitenkin olla yksityisellä sektorilla, jossa vastaavia velvoitteita, varsinkaan näitten kaikkein kriittisimpien alojen ulkopuolella, ei ole ehkä systemaattisesti asetettu niin mallimaa Suomessa kuin muuallakaan Euroopassa. Siksipä meillä oli ensimmäisenä Euroopassa käytössä kyberturvallisuusseteli, melko vaatimattomalla summalla eli muistaakseni kuuden miljoonan euron edestä haettavana isoille ja pienille yrityksille selkeitä avustuksia siten, että ne joutuivat itse maksamaan suurimman osan näistä kunnianhimoisista kyberturvallisuuden parantamishankkeistaan, mutta kuitenkin valtio tuli siinä vastaan. Tämä oli jo melko lailla aikaisemmin kuin kyberturvallisuuskeskus ENISA lähti omaa rahoitusmalliaan rakentamaan, ja Euroopassa ihaillen katsottiin tätä, että pystyttiin näin konkreettisesti auttamaan yrityksiä, huolehtimaan siitä, että ne eivät ole kyberturvallisuuden heikoin lenkki. Ja jotain tämän avustuksen tarpeesta kertonee se, että ne hakemukset täyttyivät päivissä — enintään puolitoista viikkoa kesti se, että ne kaikki oli jo jouduttu myöntämään. Siksi kysymys ehkä kuuluu, kannattaisiko tätä jo olemassa olevaa mallia, jo hyväksi havaittua mallia, jo tarpeelliseksi havaittua mallia ja kansainvälisesti arvostettua mallia jatkaa.

Puhemies Jussi Halla-aho: Kiitoksia. — Haluaako ministeri Ranne vielä vastata? — Olkaa hyvä, kaksi minuuttia.

16.09 **Liikenne- ja viestintäministeri Lulu Ranne** (vastauspuheenvuoro): Arvoisa puhemies! Lyhyesti: Tähän voi todeta, että kun meillä on nyt tämä päivitetty kyberturvallisuusstrategia ja niukat resurssit, niin tietenkin me tarkastelemme sitä, mikä olisi se tehokkain tapa saada parannettua sitä yksityisen puolen kyberturvallisuutta. Kaikki mahdollisuudet ovat meillä tässä käytettävissä.

Riksdagen avslutade debatten.

Punkt i protokollet PR 41/2025 rd

Riksdagen remitterade ärendet till kommunikationsutskottet.