Lausuntoyhteenveto
17.08.2021

Valtioneuvoston periaatepäätös kyberturvallisuuden kehittämisohjelmasta

Lausuntopyyntö

Liikenne- ja viestintäministeriö pyysi lausuntoja Kyberturvallisuuden kehittämisohjelmasta ja lausunnot pyydettiin antamaan vastaamalla lausuntopalvelu.fi:ssä julkaistuun lausuntopyyntöön. Lausuntoa ei tarvinnut lähettää erikseen sähköpostitse tai postitse. Lausuntopalautteen käsittelyn helpottamiseksi LVM pyysi, että lausunto jaotellaan lausuntopyynnössä esitettyjen väliotsikoiden mukaisesti. Lausunnon ovat voineet antaa myös muut kuin lausuntopyynnön jakelussa mainitut tahot. Lausuntokierros pidettiin 13.1.2021 – 3.2.2021.

Lausunnot ovat saatavilla osoitteessa: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=e09805fc-83a1-4207-8f16-55a991363d0d.

Yleistä lausunnoista

Lausuntoja annettiin yhteensä 55 kappaletta, ja kolme näistä lausunnoista annettiin yksityishenkilöiden toimesta. Teknologiateollisuus yhtyi lausunnossaan täysimääräisesti Finnish Information Security Cluster – Kyberala ry:n lausuntoon ja TietoEVRY Oyj yhtyi Elinkeinoelämän Keskusliitto EK:n ja Kyberala ry:n lausuntoon.

Lausunnon antoivat:

1. Bittium Wireless Oy
2. Cinia Oy
3. CSC-Tieteen tietotekniikan keskus Oy
4. Cyberwatch Finland
5. CySec Ice Wall Oy
6. Digi- ja väestötietovirasto
7. Electronic Frontier Finland - Effi ry
8. Elinkeinoelämän keskusliitto EK
9. Finnish Information Security Cluster – Kyberala ry
10. F-Secure Oyj
11. Helsingin yliopisto
12. Huoltovarmuuskeskus
13. Insta DefSec Oy
14. Internet-käyttäjät ikuisesti - IKI ry
15. Jyväskylän yliopisto
16. Liikenteenohjausyhtiö Fintraffic Oy
17. Microsoft Oy
18. MPK Maanpuolustuskoulutusyhdistys
19. Naisten Valmiusliitto
20. Netox Oy
21. Oikeusministeriö
22. Oikeusrekisterikeskus
23. Opetus- ja kulttuuriministeriö
24. Opetushallitus
25. Oulun yliopisto
26. Pelastakaa Lapset ry
27. Poliisihallitus
28. Puolustusministeriö
29. Puolustusministeriö, Turvallisuuskomitean sihteeristö
30. Puolustusvoimien pääesikunta
31. Sisäministeriö
32. Suojellaan Lapsia ry

33. Suojelupoliisi
34. Suomen Erillisverkot Oy
35. Suomen Internet-yhdistys, SIY ry
36. Suomen Kuntaliitto ry
37. Suomen Punainen Risti
38. Teknologian tutkimuskeskus VTT Oy
39. Teknologiateollisuus ry
40. TietoEVRY Oyj
41. Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry
42. Tietosuojavaltuutetun toimisto
43. Tietoturva ry
44. Traficom
45. Turun kaupunki
46. Turun yliopisto
47. Työ- ja elinkeinoministeriö
48. Ulkoministeriö
49. Valtioneuvoston kanslia
50. Valtiovarainministeriö
51. Valtori
52. Wärtsilä
53. Yksityishenkilöt

Yleiset havainnot lausunnoista

Kyberturvallisuuden kehittämisohjelmaa pidetään erittäin tärkeänä ja toivottuna, ja esitetyt kehittämistoimet nähdään yleisesti ottaen kannatettavina. Myös toteuttamistapaa pidetään yleisesti onnistuneena. Lausunnoissa esitetään myös laajaa halua ja kykyä osallistua toimenpideohjelman käytännön toteuttamiseen yhteistyössä muiden toimijoiden kanssa. Lausunnoissa korostetaan nykyisen ohjelman ja siihen mahdollisesti tulevaisuudessa lisättävien uusien toimenpiteiden riittävän rahoituksen tärkeyttä, ja monet lausunnonantajat pitävät ohjelman rahoitustasoa sen laaja-alaisuuteen ja keskeiseen rooliin nähden matalana. Lausunnoissa tuodaan myös esille, että kehittämisohjelman toimeenpanon riittävä resursointi on turvattava ja siihen on ohjattava pitkäaikaista lisärahoitusta eri lähteistä. Resurssien riittävyyden turvaamiseksi kehotetaan siirtämään painopiste erityisesti kyberturvallisuuden uhkien ja hyökkäysten ennakointiin reagoinnin sijaan, jotta vahingoilta vältyttäisiin. Lausunnoissa korostetaan myös kansallisen ja kansainvälisen yhteistyön merkitystä, ja erityisesti EU-edunvalvonnan roolia nähdään tarpeelliseksi painottaa enemmän ohjelmassa.

Koulutuksen osalta lausunnoissa nousee esille tarve panostaa laaja-alaiseen kyberturvallisuusosaamiseen, jossa huomioidaan huippuosaajien ja asiantuntijoiden lisäksi myös tavalliset työntekijät ja kattava kansalaisosaaminen. Ohjelman toimeenpanoon kiinnitetään runsaasti huomiota, ja toimenpiteet nähdään monelta osin korkeatasoisena. Tähän liittyen lausunnoissa tuodaankin esiin tarvetta tehdä tarkennuksia toimenpiteisiin niiden konkreettisuuden lisäämiseksi ja toimeenpanon selkeyttämiseksi. Erityisesti tavoitteiden saavuttamisen mittareihin kaivataan enemmän konkreettisuutta, jotta tavoitteiden saavuttamista tai saavuttamatta jättämistä voidaan arvioida onnistuneesti. Toimenpide-ehdotuksista erityisesti toimenpiteestä 12.3 lausutaan runsaasti, ja vaikka sitä myös kannatetaan usean tahon toimesta, niin useat lausunnonantajat pitävät sitä myös ongelmallisena, ja siihen kaivattaisiin esimerkiksi lisää tarkennuksia. Käsitteiden määrittelyyn kiinnitetään huomiota usean lausunnonantajan toimesta ja nähdään, että keskeisten termien, kuten kyberturvallisuuden tarkempi määrittely edistäisi kehittämisohjelman kokonaisuuden hahmottamista.

Teemakohtaiset lausunnot

Huippuluokan osaaminen

Lausunnoissa korostetaan kyberturvallisuuden asiantuntijapulaa Suomessa ja tuodaan esiin erityisesti uusien teknologioiden, kasvaneen sääntelyn ja tietoverkkorikollisten ja muiden toimijoiden lisääntyneen aktiivisuuden kasvattavan tarvetta hyödyntää alan asiantuntijoita. Huippuluokan osaaminen nähdäänkin monessa lausunnossa kehittämisohjelman tärkeimpänä painoalueena. Osaamisen kehittämisen laaja-alaista lähestymistapaa pidetään kannatettavana, ja kiinnitetään huomiota siihen, että huippuosaajien lisäksi tarvitaan myös käytännönläheistä kansalaisten kouluttamista ja kattavaa osaamista. Kattavan osaamisen edistämisessä korostetaan riittäviä resursseja, sekä laajan rekrytoinnin merkitystä sukupuoleen katsomatta. Lisäksi pidetään tärkeänä tukea yhteistyötä niiden tahojen kanssa, jotka tukevat huippuosaajien ja kansalaisten ruohonjuuritason osaamista. Myös huippuosaajien houkuttelemisen ja kansainvälisen verkostoitumisen merkitystä painotetaan.

Laajan osaamisen edistämiseksi nähdään tarpeellisena laajentaa perustason kyberturvallisuusosaaminen koskemaan kaikkia korkeakoulututkintoja. Lisäksi tuodaan esiin, että koulutusmallin kehittämisessä tulisi hyödyntää korkeakoulujen lisäksi myös yrityksiä ja muita alan toimijoita. Lausunnoissa nähdään, että osaamisen kehittämisessä voitaisiin hyödyntää myös oppisopimuskoulutusta ja harjoitteluohjelmia. Digi- ja väestötietovirasto esittää, että kansalaisten kouluttaminen voisi näkyä myös pääteeman otsikossa. Jyväskylän yliopisto ehdottaa, että perustettaisiin tutkinto-opintojen koordinointia edistävä yhteistyöfoorumi, jotta ohjelman tavoitteet voitaisiin saavuttaa. Lausunnoissa painotetaan myös muuntokoulutuksen merkitystä, jonka avulla työelämässä jo olevilla olisi mahdollisuus siirtyä aloille, joilla osaajia tarvitaan. Lausunnoissa toivotaan myös, että puolustusvoimien kyberturvallisuuden alalla tekemä koulutustyö huomioitaisiin osana kansallista osaamisen kehittämistä. Lisäksi nähdään tarpeellisena, että kyberturvallisuuden eri toimijoiden osaamistarpeet huomioidaan kaikilla osa-alueilla, myös perinteisten teknisten kompetenssialueiden ulkopuolella. Esitetään, että ohjelmassa tulisi koulutuksen uudistamisen osalta puhua koulutusohjelmista koulujärjestelmän sijaan.

Opetus- ja kulttuuriministeriö näkee, että ohjelmassa esitetyt tavoitteet kyberturvallisuuskoulutuksen kehittämisestä varhaiskasvatuksessa ja perusopetuksessa sisältyvät jo nyt varhaiskasvatussuunnitelmaan ja OKM tuo esiin tähän liittyvän OKM:n käynnistämän Uudet lukutaidot -ohjelman. OKM näkee, että opetussuunnitelmien uudistamisessa olisi tärkeä toteuttaa myös nykytilanteen kartoitus. OKM esittää, että kyberturvallisuuden koulutuksen kehittäminen -osioon lisättäisiin mukaan lukiokoulutus ja ammatillinen koulutus, ja kehottaa panostamaan kansainväliseen verkostoitumiseen. Lisäksi OKM näkee tarvetta lisätä vapaan sivistystyön roolia ohjelmassa. Naisten ja tyttöjen kannustamista kyberalalle pidetään erittäin kannattavana. Huoltovarmuuskeskus kiinnittää kuitenkin huomiota siihen, että alalle rohkaiseminen tulisi aloittaa jo varhaiskasvatuksessa, ja sen tulisi koskea koko ikäpolvea. OKM näkee hyödyllisenä panostaa myös muiden aliedustettujen ryhmien kuin naisten kannustamiseen kyberturvallisuusalalle. EK puolestaan pitää tärkeänä houkutella alalle opiskelijoita laajemmin, ja erityisesti ei-perinteisen taustan omaavien opiskelijoiden kiinnostuksen herättämiseen tulisi panostaa. Microsoft puolestaan korostaa roolimallien merkitystä tyttöjen houkuttelemisessa tieteen ja teknologian alalle. Microsoft korostaa myös kansalaisten tietoisuuden kasvattamisen merkitystä ja ilmoittaa olevansa mukana tässä prosessissa.

Cyberwatch näkee tärkeäksi panostaa tutkintopohjaisen koulutustarjonnan lisäksi joustavaan täydennyskoulutukseen ja elinikäistä oppimista tukevaan kurssi- ja koulutustarjontaan. Lisäksi se painottaa kolmea kyberosaamisen kehitystarvetta, jotka liittyvät tutkimukseen panostamiseen, päättäjien ymmärryksen lisäämiseen ja kansallisen kyberoppimispolun luomiseen. Poliisihallitus näkee viranomaisten oman osaamisen kasvattamisen erittäin tärkeänä. Naisten Valmiusliitto kiinnittää huomiota järjestöjen rooliin kansalaisten kyberturvallisuusosaamisen kehittämisessä. Suomen Punainen risti SPR kiinnittää huomiota siihen, miten kansalaisten kyberosaamisen kehittämisessä huomioidaan heikot digitaidot omaavien haavoittuvien ryhmien tarvitsema tuki. Lisäksi SPR painottaa, että järjestöt eivät voi korvata viranomaistahoja kansalaisten kyberturvallisuuden kehittämisessä ja kiinnittää huomiota järjestöjen riittävien resurssien turvaamiseen.

Lausunnoissa kiinnitetään myös huomiota siihen, että kyberturvallisuuden tuominen opetukseen entistä laajemmin vaatii merkittävää resursointia. Kuntaliitto korostaa kuntien ja kuntia lähellä olevien toimialojen kyberturvaosaamisen merkitystä ja tuo esille, että koulutuksen vahvistamisen edellyttämät lisäresurssit tulee rahoitusperiaatteen mukaisesti korvata kunnille täysimääräisenä. Turun yliopisto tuo esiin sen merkittävän roolin kyberturvallisuuskoulutuksen tarjonnassa ja näkee, että alan yliopistokoulutuksen lisäresursointi voisi helpottaa osaajapulaa tarjoamalla koulutuspaikkoja entistä laajemmalle määrälle alasta kiinnostuneita osaajia. Helsingin yliopisto näkee myös kyberturvallisuuden tutkimusrahoituksen määrän liian alhaisena. Turun yliopisto näkee, että alakohtainen kohdennettu taloudellinen tuki kilpailukykyisiin palkkauksiin yliopistoissa mahdollistaisi nykyistä paremmin parhaiden osaajien kotimaisen ja kansainvälisen rekrytoinnin tutkimus- ja koulutustehtäviin. Lisäksi Jyväskylän yliopisto kiinnittää huomiota korkeakoulujen rahoitusmalliin, jonka ei nykyisessä muodossaan nähdä edistävän yhteistoimintaa koulutuksen toteutuksessa.

Lausunnoissa kiinnitetään myös huomiota kansainvälisten huippuosaajien houkuttelemisen tärkeyteen. EK näkee, että maahanmuutto on avainasemassa osaajapulan paikkaamisessa lyhyellä aikavälillä, ja se näkee yksistään koulutuksen kehittämisen liian hitaana ratkaisuna. F-secure tuo esiin, että huippuosaajien lisäksi Suomeen voitaisiin houkutella myös vähemmän aikaa alalla olleita ulkomaisia työntekijöitä. F-secure näkee myös, että kyberturvallisuusalalla tarvittaisiin lisää osaamista EU-rahoitusvälineisiin liittyen. Oulun yliopisto näkee kyberturvallisuuskoulutuksessa kouluttajien koulutuksen mahdollisena pullonkaulana ja kiinnittää huomiota tarpeeseen lisätä kouluttajien määrää. CSC-Tieteen tietotekniikan keskus näkee työharjoittelujaksoihin liittyvässä yhteistyössä tarvetta konkreettisemmille toimenpiteille, ja CSC:n mielestä osaamissertifiointeihin tulisi panostaa erityisesti avainhenkilöiden kohdalla.

Helsingin yliopisto kiinnittää huomiota avointen verkkokurssien hyödyntämisen osana kyberturvalliskoulutuksen kehittämistä. Helsingin yliopiston mielestä yhteiskunta- ja käyttäytymistieteellinen tietoperusta tulisi huomioida kyberturvallisuuden koulutustarpeissa. FiCom ry näkee tarvetta panostaa myös kyberjohtamisen kouluttamiseen. FiCom ry näkee myös tärkeänä, että yritysten ulkopuolelta tapahtuvalla operatiivisella johtamisella ei vaaranneta olemassa olevia toimintoja, ja että koulutuksista viestimisessä käytetään eri kohderyhmille kohdennettua viestintää. Pelastakaa Lapset ry näkee, että lasten suojelemiseen digitaalisen yhteiskunnan vaaratilanteissa tarvitaan erityistä osaamista niin julkisella, kuin yksityiselläkin sektorilla. Maanpuolustuskoulutusyhdistys tuo esiin, että sillä on kattavaa kokemusta ja osaamista kyberturvallisuuden koulutus- ja harjoitustoiminnasta. MPK esittää harkittavaksi

jatkosuunnittelussa selkeän koulutussuunnitelman laatimista avaamaan käytännön esimerkein osaamisen koulutuspolkuja ja eri mahdollisuuksia. Puolustusvoimat näkee, että osana yhteiskunnan kyberturvallisuuden huippuosaamisen kehittämistä tulee huomioida myös asevelvollisuuden aikana joko varusmiehenä tai reserviläisenä hankitun kokemuksen luomat mahdollisuudet nykyistä laajemmin. Puolustusvoimien mielestä tämä tulisi kirjata kehittämisohjelmaan vähintään yhdeksi mittariksi.

Kiinteä yhteistyö

Yritysten, tutkimuslaitosten, sekä julkisten toimijoiden välinen yhteistyö nähdään avainasemassa kyberturvallisuuden kehittämisessä sekä tavoitellun kyberturvallisuuden ekosysteemin luomisessa. Lausunnoissa painotetaan myös kansainvälisen kyberturvallisuusyhteistyön merkitystä ja nähdään, että Suomen tulisi tehostaa vaikuttamista kansainvälisellä tasolla ja erityisesti EU:ssa. Lausunnoissa tuodaan myös esiin, että kansainvälisen yhteistyön muodot olisi hyvä määritellä niin, että työn- ja tiedonjako toteutetaan selkeästi ja kotimaista ekosysteemiä palvelevasti. Lausunnoissa korostettiin myös yhteisen harjoitustoiminnan merkitystä ja sitä, että harjoitustoimintaan olisi tärkeää saada mukaan nykyistä laajempi joukko yrityksiä.

Helsingin yliopisto kiinnittää huomiota etäyhteyksien hyödyntämisen kasvun mukanaan tuomiin mahdollisuuksiin kansainvälisessä yhteistoiminnassa ja näkee yhteyksien pitämisen EU:n osaamiskeskittymiin tärkeänä osana yhteistoiminnan edistämistä. F-secure esittää, että Suomeen tarvittaisiin kyberturvallisuusyhteistyöhön erikoistuneita pysyvämpiä rakenteita ja foorumeita. Valtioneuvoston kanslia pitää tärkeänä, että ohjelmassa tuotaisiin esille Suomen aktiivinen osallistuminen EU:n kyberturvallisuuden kehittämiseen. Insta DefSec Oy näkee, että jatkossa tarvittaisiin esitettyäkin vahvempi panostus harjoitustoimintaan. Insta DefSec Oy näkee myös, että harjoitustoimintapalveluidenkin osa-alueella tulisi edistää uusia skaalautuvia ja kaupallista potentiaalia omaavia innovaatioita kansallisiin ja kansainvälisiin tarpeisiin.

Puolustusvoimat pitää tärkeänä, että osaamisen kehittämisessä ja harjoitustoiminnassa huomioidaan kunkin kyberviranomaisen erityistarpeet ja että harjoittelua suoritetaan eri valmiustilojen skenaarioissa niiden erityistarpeet huomioiden. Pelastakaa Lapset ry näkee, että harjoitustoiminnassa on osana kriittisten arvoketjujen suojaamista huomioitava myös lasten turvallisuuteen ja oikeuksiin liittyvät kysymykset. Harjoitustoiminnan osalta pidetään perusteltuna, että oppilaitokset mainittaisiin tarpeellisina yhteistyötahoina. Lisäksi kiinnitetään huomiota tarpeeseen varmistaa oppilaitosten pääsy ohjelmassa mainituille harjoitusympäristöille kohtuullisin resurssein. Lisäksi EK kiinnittää huomiota harjoituksista kertyvien havaintojen analysointiin ja viestintään. Maanpuolustuskoulutusyhdistys MPK pitää kaikkia erilaisia harjoitusskenaarioita palvelevan yhden tai useamman valtakunnallisen harjoitusympäristön rakentamista haasteellisena tai jopa mahdottomana. MPK näkeekin, että olisi todennäköisesti parempi rakentaa useampia pienempiä erillisiä ympäristöjä, jotka verkotettaisiin toimimaan yhdessä aina skenaarioiden vaatimusten mukaan.

Lausunnoissa nähdään myös tarpeellisena varmistaa, että strategisia kumppanuussuhteita syntyy, ja että viranomaisten välinen operatiivinen yhteistyö on tehokasta ja hyvin optimoitua. Oikeusrekisterikeskus näkee, että Disobeyn GovTrack olisi tehokas väline viranomaisten välisen yhteistyön kehittämiseen. Oikein suunnattu harjoitusyhteistyö sekä lainsäädän-

nölliset selvitykset nähdään myös avainroolissa. Yhteistyöfoorumin perustamista ehdotetaan myös kiinteän yhteistyön edistämiseksi. Jyväskylän yliopisto näkee tutkimustuloksien kaupallistamisen edellyttävän soveltuvien rahoitusinstrumenttien olemassaoloa, ja Jyväskylän yliopisto pitää entisen Tekesin aiempia tavoitetutkimusohjelmia hyvänä esimerkkinä soveltuvista rahoitusinstrumenteista. Lisäksi Jyväskylän yliopisto kiinnittää huomiota nykyisiin Business Finlandin ja Akatemian tutkimusrahoitushakuihin, jotka se näkee äärimmäisen raskaina ja työläinä. Jyväskylän yliopisto ei pidä myöskään OKM:n nykyistä resurssimallia soveltuvana.

Nähdään, että valtionhallinnon digitaalisten palveluiden turvallisuuden varmistamisen tulisi koskea koko julkishallintoa. Lisäksi kiinnitetään huomiota kyberturvallisuuden tärkeyteen myös normaalioloissa. Teema-aiheisten yhteistyöryhmien perustamista pidetään kannatettavana ja nähdään, että ryhmien tulisi olla vahvasti poikkihallinnollisia. Puolustusvoimat näkee, että asevelvolliset ovat kyberpuolustuksen keskeisin suorituskyky. Myös Cyberwatch pitää tarpeellisena hyödyntää Suomen asevelvollisuusjärjestelmää ja puolustusvoimia tehokkaammin ja se näkee viranomaisten ja elinkeinoelämän välisessä yhteistyössä kehitettävää. Poliisihallitus haluaa lisätä turvallisuusviranomaisten koordinoituja harjoituksia. Lisäksi poliisihallitus kannattaa kyberturvallisuuden vaatimusten yhdenmukaistamista ja niiden täyttymisen valvontaa, sekä esittää tälle jatkokehitysmahdollisuuksia KATAKRI2020 työn pohjalta. Poliisihallitus painottaa myös tietojärjestelmien ja tietovarantojen yhdenmukaisen vaatimuskehikon merkitystä. Suomen Punainen Risti näkee, että onnistunut yhteistoiminta edellyttää sujuvaa tilannekuvan jakamisen mallia viranomaisten, järjestöjen ja elinkeinoelämän välillä.

F-secure näkee, että Suomesta löytyvää kyberturvallisuusosaamista tulisi hyödyntää lainsäädäntötyössä entistä tehokkaammin. CSC pitää tärkeänä, että Haukka-toimeenpanosuunnitelma ja Digitaalinen Turvallisuus 2030 -hankkeen välinen yhteistoiminta on saumatonta. Puolustusvoimat tuo esiin, että koska kyberturvallisuuden kehittämisohjelma toteuttaa nimenomaan kansallista kyberturvallisuusstrategiaa, sen olisi syytä analysoida tarkemmin koko kansallisen kehittämisen kokonaisuus. Helsingin yliopisto näkee yhteiset kyberharjoitusympäristöt tärkeänä. Kuntaliitto huomauttaa, että yhteistyön mahdollistamiseksi tulisi huolehtia salassapidettävien tietojen luovuttamiskäytäntöjen tarkistamisesta, mikä voi edellyttää lainsäädäntömuutoksia. Kuntaliitto pitää myös kuntien tiedonsaannin turvaamista mahdollisissa häiriötilanteissa ensiarvoisen tärkeänä.

Turun yliopisto painottaa ihmisnäkökulman merkitystä kyberturvallisuudessa ja näkee, että kyberturvallisuuden suunnitteluun pitäisi saada myös käyttäjien näkökulma. Turun yliopisto ehdottaa, että Suomeen pitäisi perustaa eri alan toimijoista muodostuva yhteinen ennakointiryhmä, joka tuottaisi aloitteita mm. lainsäädännön ja yhteiskunnan prosessien puolelle. FiCom ry näkee, että julkisen ja yksityisen sektorin välinen kommunikointi tarvitsee turvallisen työkalun, jota voitaisiin mahdollisesti käyttää myös yksityisten toimijoiden välisessä yhteydenpidossa. Naisten Valmiusliitto ry korostaa järjestöjen yhdistävää roolia kansalaisten ja viranomaisten välisessä yhteistyössä. Naisten Valmiusliitto ry näkee myös, että ohjelmassa olisi hyvä tuoda esiin selkeämmin kolmannelle sektorille osoitettu koordinoiva vastuutaho kyberturvallisuuskeskuksesta, jotta olemassa oleva tieto ja resurssit saataisiin parhaiten hyödynnettyä.

Puolustusvoimien mielestä kehittämisohjelmassa ei ole kuvattu toimenpiteitä, joilla riittävällä tasolla parannettaisiin reagointikykyä nopeisiin kansallista turvallisuutta uhkaaviin tilannekehityksiin. Puolustusvoimat esittää, että operatiivisen viranomaisyhteistoiminnan kehittäminen tulee lisätä kehittämistoimenpiteeksi. Suomen Internet-yhdistys SIY ry kiinnittää huomiota siihen, että kansainvälisessä yhteistyössä kyberturvallisuustyötä tehdään myös yhteisöissä, jotka eivät ole valtiosidonnaisia, ja että näiden yhteisöjen toimintaan osallistuu myös suomalaisia toimijoita. SIY ry esittää, että kehitysohjelmaan lisättäisiin yhteistyötahoksi myös kansainväliset verkostoyhteisöt ja niitä edustavat kansalliset organisoituneet yhteisöt. Tietosuojavaltuutetun toimisto näkee, että osana kiinteän yhteistyön pääteemaa olisi hyvä huomioida myös aktiivinen osallistuminen ja vaikuttaminen kansalliseen ja kansainväliseen tietosuojayhteistyöhön erityisesti tietosuojaneuvostossa. Tietosuojavaltuutetun toimisto pitää tärkeänä, että tietosuojavaltuutetun toimisto voisi jatkossa osallistua entistä tiiviimmin valvontaviranomaisten yhteistyöhön erityisesti siltä osin, kun yhteiskunnallisten haavoittuvuuksien syitä arvioidaan ja niitä pyritään ennaltaehkäisemään.

Vahva kotimainen kyberturvateollisuus

Lausunnoissa painotetaan kyberturvateollisuuden menestymisen välttämättömyyttä ohjelman pääteemojen toteutumisen kannalta sekä kiinnitetään huomiota kansainvälistymisen edistämiseen. Kotimaisten kyberturvatuotteiden ja -palveluiden kasvun ja kansainvälistymisen tukemista pidetään Suomen kannalta tärkeänä erityisesti työllisyyden ja talouskasvun näkökulmasta. Lisäksi nähdään tarpeellisena panostaa uusien kyberturvayritysten lisäksi myös jo olemassa oleviin kyberturvallisuusalan toimijoihin, ja erityisesti ohjelman keskittyminen pk-yrityksiin nähdään paikoittain ongelmallisena isompien yritysten kannalta. Lausunnoissa korostetaan myös julkisten hankintojen merkitystä kansallisen kyberturvallisuuden vahvistamisen kannalta ja nähdään, että kriittisten järjestelmien kohdalla hankintakriteereissä tulisi huomioida myös kansalliset turvallisuusnäkökohdat.

Cyberwatch näkee tarvetta selkeämmille tavoitteille, sekä toimenpiteille näiden tavoitteiden saavuttamiseksi. Cyberwatch korostaa myös kansallisen koordinoinnin ja resursoinnin roolia. Kyberturvallisuusalan kasvustrategian laatimista pidetään tärkeänä. Myös kansallisen kasvu- ja osaamiskeskuksen perustamista kannatetaan. Kyberalan mukaan sekä strategian laadinnassa, että kasvu- ja osaamiskeskuksen toiminnassa on huomioitava alan yleisten kasvuedellytysten edistäminen, innovaatioiden tuotteistaminen sekä niiden myynnin ja markkinoinnin vahvistaminen, Suomen houkuttelevuus investointikohteena sekä kansallisten ja EU:n kyberturvallisuuspanostusten mahdollisuuksien täysimääräinen hyödyntäminen Suomessa. Kyberala pitää kannatettavana suomalaisten kyberturvallisuustuotteiden ja –palveluiden mahdollisimman laajaa hyödyntämistä. Kyberalan mukaan palveluiden onnistuneeseen hankintaan tarvitaan lisää osaamista, ja se näkee, että julkishallinnon tehokkaan ja taloudellisen ostotoiminnan sekä innovatiivisten hankintojen kehittämiseen olisi syytä panostaa. Kyberala korostaa myös kansainvälisen kilpailukyvyn merkitystä, ja näkee kilpailukyvyn parantamisessa avainroolissa viennin edellytyksiin liittyvien rakenteiden toimivuuden arvioinnin.

Teknologian tutkimuskeskus korostaa resursoinnin merkitystä kotimaisen IPR-portfolion kehittämisessä. Riittävään resursointiin kiinnitetään huomiota myös yleisellä tasolla kotimaisen kyberturvateollisuuden kehittämisessä. F-secure tuo esiin Suomen vahvuuden meriturvallisuuden alalla ja esittää, että Suomi voisi erikoistua myös näiden alojen kyberturvallisuuskysymyksiin. Helsingin yliopisto korostaa yliopistojen tärkeää roolia uusien innovaatioiden

luonnissa ja haluaisi, että tohtorikoulutettavien ja maisterivaiheen opiskelijoiden verkostoitumiseen alan toimijoiden kanssa panostettaisiin esimerkiksi harjoittelujaksojen avulla. EK ehdottaa osaajahubien perustamista pienten mikroyritysten kehittymisen edistämiseksi.

Huoltovarmuuskeskus korostaa laajan kyberturvaosaamisen merkitystä kotimaisen kyberturvateollisuuden menestyksessä, ja erityisesti sitä, että myös muiden tahojen kuin varsinaisen teknologian kehittäjien osaamisen tulisi panostaa. Suomen Internet-yhdistys korostaa, että teollisuuden elinvoimaisuus syntyy vain myynnin kautta. Myyntitaitoihin, asiakaskohtaamiseen, myyntiprosessin ja asiakaskokemuksen johtamiseen tarvitaan Suomen Internet-yhdistyksen mielestä enemmän panostusta, kuin mitä kehittämisohjelmassa esitetään. Pelastakaa Lapset ry tuo esille, että mainitussa kansallisessa koordinaatiokeskuksessa tulisi olla myös lasten kyberturvallisuuteen liittyvää substanssiosaamista. Puolustusvoimat painottaa kotimaisen kyberturvallisuuden merkitystä valtion huoltovarmuuden, sekä kriisinsietokyvyn kannalta. CySec Ice Wall Oy näkee tarpeelliseksi muuttaa lainsäädäntöä niin, että se mahdollistaa primääridatan käyttämisen kotimaisessa kyberturvatuotekehityksessä. Suomen Erillisverkot tuo esille, että ulkomaalaisten yritysostosta annetun lain mukaisiin tilanteisiin tulisi pyrkiä varautumaan jo ennakolta ja turvata Suomen kannalta kriittiset kyberturvatuotteet ja -palvelut jo tuotekehitysvaiheessa.

Tehokkaat kansalliset kyberturvakyvykkyydet

Lausunnoissa pidetään ehdotettuja kehittämistoimenpiteitä kannatettavina ja erityisesti AQUA-statuksen saavuttamista pidetään erinomaisena tavoitteena. Kyberturvallisuuden ekosysteemiin luomista pidetään myös kannatettavana, ja tehokkaan kyberpuolustuksen vaatimuksiin erityisesti lainsäädännön kannalta kiinnitetään huomiota. Useat lausunnonantajat kiinnittävät kuitenkin huomiota ohjelman toimenpiteiden ja erityisesti AQUA-statuksen saavuttamisen edellyttämiin resursseihin ja pitkäjänteiseen yhteistyöhön. Puolustusministeriö puolestaan painottaa, että AQUA-kyvykkyyden vaatima syväosaaminen edellyttää kaikkien kansallisten kryptotoimijoiden tiivistä yhteistyötä, ja että puolustusvoimiin jo rakennettu kryptokyvykkyys tulisi hyödyntää. Puolustusvoimat näkee, että Puolustusvoimien tulisi olla mukana nimettynä toimijana AQUA-kyvykkyyden saavuttamisen osalta. Puolustusvoimat näkee kuitenkin, että AQUA-statuksen rakentaminen käytössä olevilla resursseilla ei vaikuta mahdolliselta.

Cyberwatch painottaa nopean toiminnan merkitystä ja näkee, että ohjelmassa tulisi olla toimenpiteet myös kansallisen kyberjohtamisen, strategisen tilannekuvan ja nopean reagointikyvyn kehittämiseen. Lisäksi Cyberwatch näkee tarvetta kokonaisvaltaiselle kyberturvalainsäädännölle ja haluaa sen osaksi kehittämisohjelmaa. Myös puolustusministeriö tuo esiin, että kyberpuolustuksen suorituskyvyn kehittäminen edellyttää kokonaisvaltaista toimivaltuustarkastelua ja sen myötä tarvittaessa käynnistettävää säädösvalmistelua. Puolustusministeriö korostaa kyberturvallisuuden ekosysteemin merkitystä osana kansallista turvallisuutta ja huoltovarmuutta, ja puolustusministeriö näkee viranomaisyhteistyön lisäksi kansallisen suvereniteetin turvaamisen olennaisena. Puolustusministeriö ehdottaa myös, että kehittämisohjelmassa selvitettäisiin laajamittaisesti aluevalvontaan, viranomaisyhteistyöhön, virka-apuun sekä voimankäyttöön kybertoimintaympäristössä liittyvät kysymykset, sekä mahdolliset toimivaltuuksiin ja lainsäädäntöön liittyvät muutostarpeet poikkihallinnollisena yhteistyönä.

Nähdään tarpeellisena panostaa salaustuotteisiin liittyvien tietoturvahyväksymisten läpivienteihin sekä kotimaassa, että kansainvälisesti. Kiinnitetään huomiota Vastaamon tietomurron osoittamiin ongelmakohtiin henkilötietojen suojaamisessa. Ohjelmassa mainittuihin huoltovarmuuskriittisiin arvoketjuihin liittyvän havainnointikyvyn parantamista pidetään erityisen tärkeänä. Microsoft tukee kyberturvallisuuden kasvu- ja osaamiskeskuksen perustamista kansallisen koordinaatiokeskuksen yhteyteen. Digi- ja väestötietovirasto DVV tuo esille, että se voisi tukea hankintoihin liittyvien turvallisuusasioiden substanssiosaamisen kehittämistä kyberturvallisuuden tuotteiden ja palveluiden ostamisessa julkisessa hallinnossa. Lisäksi DVV tuo esiin, että yhteiskunnan kriittisten tietovarantojen, palveluiden ja järjestelmien selvitystyö julkisen hallinnon järjestelmien osalta voitaisiin mahdollisesti toteuttaa DVV:n toimeenpanemana. DVV esittää myös, että kriittisten palveluiden turvallisen ohjelmistokehitysprosessin kehittäminen ja siihen kytkeytyvän ohjeistuksen kehittäminen voitaisiin toteuttaa soveltuvin osin DVV:ssä. CSC näkee tarpeelliseksi harmonisoida tiedon suojausvaatimuksia ei-luokitellun tiedon osalta ja CSC:n mukaan harkiten annettavalle tiedolle tulisi määritellä KATAKRI-kriteeristöä joustavammat kriteerit. Lausunnoissa kiinnitetään myös huomiota tarpeeseen sisäänrakentaa tietoturva kansalliseen infrastruktuurin.

CySec Ice Wall Oy tuo esille, että kaikkien kriittisten palvelimien tietoliikenneyhteydet tulisi varustaa kyvykkyydellä yhdistää tutkittavuus- ja todistettavuusjärjestelmä, jotta mahdollisen tutkinnan alkaessa voidaan nopeasti palata tutkimaan vanhoja tietoliikennetapahtumia. Oikeusrekisterikeskus näkee, että Traficomille voisi osoittaa myös muita tehtäviä kuin fi-verkkotunnukseen liittyvät tehtävät. Huoltovarmuuskeskus kiinnittää huomiota tarpeeseen huomioida kasvavan datatalouden ja siihen liittyvät kyberturvallisuusvaatimukset. Insta DefSec Oy tiedustelee ”kansallisen salaustuoteperheen” määritelmää, mutta ei kuitenkaan pidä liian tarkkaa määrittelyä tarkoituksenmukaisena teknologian nopean kehittymisen takia. Insta DefSec Oy näkee myös järkevänä hyödyntää jo olemassa olevaa osaamista ja resursseja uuden rakentaminen sijasta. Pelastakaa Lapset ry näkee, että väkivaltaisten ääriryhmien verkkoympäristöissä harjoittama toiminta ja sen aiheuttamat uhat yhteiskunnan turvallisuudelle tulisi huomioida. Cinia Oy korostaa selkeän johtamismallin sekä yksityisen sektorin monipuolisen hyödyntämisen merkitystä.

Puolustusvoimat näkee tarpeelliseksi selvittää ohjelmassa, mitkä yhteiskunnan toiminnan kannalta tärkeät kybertoimintaympäristön toimenpiteet ja vastuut ovat kunnossa, mitkä jäävät tekemättä ja missä on päällekkäisyyttä. Puolustusvoimat korostaa myös, että sen täytyy voida itsenäisesti hoitaa kriittisimmät kyberpuolustuksen tehtävät ja luoda niihin kyvykkyydet, eikä ohjelman toteuttaminen saa vaarantaa tätä. Puolustusvoimat näkee, että kansallinen kryptostrategiatyö ja kansallisen krypto-osaamisen kehittäminen tulisi rakentaa Puolustusvoimien fasilitoiman strategiatyön ja Puolustusvoimissa kehitettävän kansallisen kryptolaboratorion osaamisen pohjalle.

Seuranta ja raportointi

Lausunnoissa pidetään tärkeänä, että kehittämisohjelman etenemiselle on asetettu selkeät mittarit, sekä raportointivastuut ja seuranta. Erityisesti toivotaan, että kehittämisohjelman toteutumisen seuranta olisi jatkuvaa, ja että ohjelman ajallinen ulottuvuus olisi riittävä. Lisäksi kiinnitetään huomiota siihen, että kehittämisohjelman pitäisi olla dynaaminen ja tarpeen vaatiessa sen sisältöä pitäisi pystyä muokkaamaan tehokkaasti. Lausunnoissa nähdään myös tarvetta julkisen ja yksityisten sektorin yhteistyölle ohjelman päivittämisessä.

Osan ohjelman tavoitteista ja mittareista nähdään myös kaipaavan enemmän konkreettisuutta.

Helsingin yliopisto korostaa kansalaisten ja yritysten rikosuhrikokemuksien mittaamisen merkitystä kyberturvallisuusosaamisen ja kyberrikollisuuden torjunnan toimien ja ohjelmien vaikuttavuuden seurannassa. Puolustusministeriö ehdottaa, että kehittämisohjelmassa käytettyihin vertaileviin mittareihin sisällytettäisiin laaja-alaista osaamisen ja kyvykkyyden mittaria, kuten National Cyber Power indexiä. Puolustusministeriö ehdottaa lisäksi, että kyberturvallisuuden sekä kansallisen kyberuhkiin varautumisen tilaa tarkasteltaisiin jatkossa kahden vuoden välein ulkopuolisen riippumattoman toimijan tekemissä raporteissa. CSC näkee, että seurannan ja raportoinnin tulisi sisältää seurantaa myös toteutetuista turvallisuusarvioinneista ja -sertifioinneista. CSC esittää lisäksi useita konkreettisia toimenpide-ehdotuksia esimerkiksi turvallisuusselvityksen teettämiseen liittyen. CSC painottaa myös yhteistoiminnan merkitystä.

Ulkoministeriö korostaa, että kvantitatiivisuuden ohella kvalitatiivisuus on tärkeä mittari kyberturvallisuuden kehittämisessä. Ulkoministeriö kiinnittää huomiota myös ohjelman eri toimenpiteiden vaatimusten ja mittaamisen eritasoisuuteen. Valtioneuvoston kanslia ehdottaa, että kansalaisten kyberturvallisuusosaamisen arviointi otetaan osaksi kansallista kyberturvallisuusmittaristoa. Valtioneuvoston kanslia kiinnittää myös huomiota tarpeeseen mitata hallinnonalojen tietoturvallisuuden tasoa aktiivisesti, jotta tietoturvallisuuden tasosta saataisiin vuosittainen selvyys. Valtioneuvoston kanslian mielestä kehitysohjelmassa tulisi myös selkeästi ilmaista tavoiteltava kyberturvallisuuden taso. Elinkeinoelämän keskusliiton mielestä olisi hyvä, jos ohjelmassa tarkasteltaisiin lyhyesti myös sitä, miten aikaisemmissa kehitysohjelmissa ja niiden tavoitteiden saavuttamisessa on onnistuttu, ja mitä nyt pyritään tekemään toisin.

Toimeenpanosuunnitelma

Oikeusministeriö OM kiinnittää huomiota ohjelman toimeenpanosuunnitelman lukuisiin vastuutahoihin ja esittää harkittavaksi, tulisiko joissakin kohdin määritellä päävastuutaho tai koordinaattori. Toimeenpanosuunnitelman 11 kohdan osalta OM näkee perusteltuna lisätä vastuutahoihin myös muut ministeriöt sekä keskeisiä palveluita tuottavat tahot. OM korostaa 11 kohtaan liittyen myös viranomaisten turvallisen tiedonvaihdon merkitystä. Valtiovarainministeriö esittää, että se poistetaan toimeenpanosuunnitelman kehittämistoimenpiteen 7.2 vastuutahoista. Ulkoministeriön mielestä olisi hyvä analysoida sitä, mitkä ohjelman toimenpiteet on järkevää toteuttaa virkatyönä, ja mitkä toimenpiteet edellyttävät projektiluontoista lähestymistapaa. Elinkeinoelämän keskusliitto EK ehdottaa, että toimenpiteessä 2.9 käytetty sanamuoto ”suomalaisen teollisuuden palvelukseen”, voitaisiin korjata sanamuodolla ”suomalaisen elinkeinoelämän palvelukseen.” Toimenpiteen 10.1 osalta EK painottaa yritysten kuulemisen merkitystä, ja näkee olennaisena, että aiheeseen liittyvät päällekkäiset EU-hankkeet huomioidaan riittävästi. Vaatimuksia säädettäessä tavoitetason saavuttamiseen käytettävien keinojen tulisi EK:n mukaan jäädä yritysten itsensä harkittaviksi.

Puolustusministeriö ehdottaa, että puolustusministeriö lisätään toimijana kehittämistoimenpiteiden kohtiin 7.1 ja 7.2. Kehittämistoimenpiteiden kohtaan 8.1 puolustusministeriö esittää lisättäväksi lainsäädännön tarkastelun, sekä valtiovarainministeriön lisäämistä vastuutahoihin. Puolustusvoimat painottaa kyberpuolustuksen näkökulmasta toimeenpanosuunnitelman 8.1 kohtaa ja näkee, että sen saavuttamisessa on keskeisessä roolissa vuoden 2013

kyberturvallisuusstrategian linjausten loppuun saattaminen. Puolustusvoimien mukaan tämä edellyttäisi muun muassa säädösvalmistelun käynnistämistä. Kehittämistoimenpiteiden kohdan 10.3 vastuutahoihin puolustusministeriö esittää turvallisuusviranomaisten lisäämistä osana kokonaisvaltaisen kansallisen kybertilannekuvan kehittämistä. Kehittämistoimenpiteiden kohdan 12.2 osalta puolustusministeriö esittää puolustusvoimien lisäämistä vastuutahoksi. Kehittämistoimenpiteiden kohdan 12.3 vastuutahoihin puolustusministeriö esittää lisättäväksi puolustusministeriön sekä sisäministeriön. Puolustusvoimat korostaa toimenpidesuunnitelman 12.3 kohdan merkitystä ja näkee, että puolustushallinnon tulee ehdottomasti olla mukana tässä työssä maanpuolustuksen tarpeiden näkökulmasta.

Huoltovarmuuskeskus HVK näkee toimeenpanosuunnitelman 1.4 kohdan tärkeänä. HVK tuo esille, että kohdan 3.1 tavoitteen saavuttaminen riippuu tavoitteesta 10.2. HVK kuitenkin näkee, että sen Digitaalinen Turvallisuus 2030 -ohjelman myötä tavoite olisi saavutettavissa. HVK näkee myös, että kohtien 10.1–10.3, sekä kohtien 11.1 ja 11.2 voidaan katsoa kuuluvan soveltuvin osin Digitaalisen Turvallisuus 2030 -ohjelman projektien toteutukseen. Kohta 12.3 on HVK:n mukaan osa sen normaalitoimintaa. Turun yliopisto näkee, että toimeenpanosuunnitelma tarvitsee lisää konkreettisuutta ja tuo esiin, että monen esitetyn toimenpiteen aikataulu on avoin. Turun yliopisto näkee myös, että toimeenpanosuunnitelman 2.1 kohdassa tulee selvittää kolme kohtaa: kansalaistaito, alakohtainen perusosaaminen ja erityisasiantuntijat. Lisäksi rahoitus tulisi Turun yliopiston mielestä kohdistaa kaikille kolmelle eri osa-alueelle. Turun yliopisto näkee myös tarvetta panostaa laajaan osaamiseen ja eri aloille räätälöityyn koulutukseen, ja esittää, että tämä huomioitaisiin toimenpanosuunnitelman kohdassa 2.6. Turun yliopisto näkee, että myös tämä vaatisi erillisen rahoituspohjan. Maanpuolustuskoulutusyhdistys MPK tuo esiin, että se on toteuttanut jo muutamien vuosien ajan käytännössä toimeenpanosuunnitelman kohtien 1.2–1.6, 2.1, 2.6-2.8, 3.1, 3.2 ja 11.1 sekä liitteen 2 kohtien 1–3 kokonaisuuksia.

Tietosuojavaltuutetun toimiston mukaan toimenpiteessä 2.1 olisi syytä pyrkiä tunnistamaan samalla myös henkilötietojen käsittelyn koulutukseen liittyvät muutostarpeet ja sisällyttää ne entistä syvemmin mukaan opetussuunnitelmiin. Lisäksi myös esimerkiksi toimenpiteen 1.6. mukaisessa kansalaisille kohdistetun kyberturvallisuustietoisuuden viestintäsuunnitelman laatimisessa olisi hyvä huomioida henkilötietojen suojaamiseen liittyvät näkökohdat. Tietosuojavaltuutetun toimisto näkee, että yhteiskunnallisten haavoittuvuuksien syitä voitaisiin arvioida ja ennalta ehkäistä ottamalla kaikki valvovat ja tutkivat viranomaiset osaksi toimenpidettä 10.3. Tietosuojavaltuutetun toimisto tuo myös esille, että osana toimenpidettä 11.2. olisi syytä arvioida myös yleisen tietosuoja-asetuksen mukaisten tietosuojasertifiointien käyttöä.

Ulkoministeriö nostaa kyberturvallisuuden johtamisen ja kansallisen koordinaation kehittämisen keskeiseksi tavoitteeksi ja näkee, että tätä tavoitetta tulisi käsitellä toimeenpanosuunnitelmassa. Kyberala haluaa varmistaa, ettei omistajuutta koskevasta toimeenpanosuunnitelman kohdasta 12.3 aiheudu häiriötä markkinoiden toimintaan. Myös F-secure ja EK kiinnittävät huomiota 12.3 kohtaan ja kaipaavat sen selkeyttämistä. Insta DefSec Oy pitää 12.3 kohdan lausetta ”Tunnistetaan kansallisesti kriittiset kyberturvayhtiöt ja turvataan niiden kansalliset omistusosuudet” monelta osin ongelmallisena ja näkee, että kansallisen turvallisuuden varmistaminen on tarkoituksenmukaisempaa toteuttaa ilman pakotetta omistuksesta. Vaihtoehtoisena ilmauksena Insta DefSec Oy esittää virkettä ”Kriittisten kybertur-

vayhtiöiden osalta tulee varmistaa, että mahdollisissa kansallisen intressin kannalta haitallisissa määräysvallan siirtymistilanteissa sopimuksin on mahdollistettu järjestelyt, joilla valtion etu voidaan turvata.”

Muita havaintoja lausunnoista

Tietoturvatason parantaminen yhteiskunnan kriittisillä alueilla nähdään erityisen tärkeänä tavoitteena kyberturvallisuuden kehittämisessä. Nähdään tarpeelliseksi avata kehittämisohjelman ekosysteemi-mallia tarkemmin. Opetus- ja kulttuuriministeriön mukaan Tilastokeskus tilastoi tutkimus- ja kehittämistoimintaa, ei tutkimus- ja kehitystoimintaa, kuten ohjelmaan on kirjattu. Poliisihallitus haluaa turvallisuusviranomaisten kyberturvallisuuden kehittämisen omaksi osakokonaisuudekseen kehittämisohjelmaan. Suomen Punainen Risti SPR korostaa kansalaisten roolia ohjelman kokonaisuudessa ja näkee, että kansalaisten avunsaantimahdollisuuksiin kyberuhkatilanteissa tulisi panostaa. Nykyisessä ohjelmassa olevia toimenpiteitä SPR pitää tältä osin riittämättöminä. SPR pitää ”valitus- ja viestintätyö” –termiä vanhahtavana, ja esittää sen korvaamista termillä ”turvallisuusviestintätyö.” SPR näkee, että kansalaisille tulisi luoda selkeät informaatiokanavat häiriötilanteita varten ja kaikkia toimijoita tulisi kannustaa avoimeen viestintään.

Valtiovarainministeriö haluaa sisällyttää johdantotekstiin neljännelle sivulle uuden muotoilun kehittämisohjelman rahoitukseen liittyen, sekä uuden lisäyksen kehittämisohjelman määrärahoista sivulle 17. Valtiovarainministeriö ehdottaa lisäksi, että kehittämisohjelmaan selvennetään NIS-ehdotuksen ja kehittämisohjelman väliset riippuvuudet. Kyberala ilmoittaa olevansa mielellään mukana kehittämisohjelman toteuttamisessa. Teknologian tutkimuskeskus kiinnittää huomiota kansallisen kyberturvallisuuden koordinaatiokeskuksen hyödyntämismahdollisuuksiin kehittämisohjelman tavoitteiden toteuttamisessa. Lausunnoissa tuotiin esille, että ohjelmassa tulisi viitata Valtioneuvoston periaatepäätökseen julkisen hallinnon digitaalisesta turvallisuudesta ja sen toimeenpanosuunnitelmaan, Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -ohjelmaan sekä TITUKRI:n loppuraportin toimenpideehdotuksiin.

Suojellaan Lapsia ry ja Pelastakaa Lapset ry kiinnittää huomiota kyberympäristön luomiin uhkiin lapsille ja nuorille, ja erityisesti seksuaaliseen häirintään ja seksuaaliseen väkivaltaan. Suojellaan Lapsia ry ja Pelastakaa Lapset ry näkevät valistuksen erityisen tärkeänä ongelman ratkaisemisessa. Suojellaan Lapsia ry kannattaa myös resurssien lisäämistä koko rikosoikeudellisessa prosessissa ja kiinnittää huomiota lainsäädännön kehittämistarpeisiin. Pelastakaa Lapset ry korostaa, että laajamittaiset, kriittiseen infrastruktuuriin kohdistuvat kyberuhkat koskettavat myös lapsia. Pelastakaa Lapset ry näkee myös, että elinkeinoelämä on avainasemassa lapsiin kohdistuvien kyberuhkien torjunnassa, ja Pelastakaa Lapset ry edellyttää valtiolta tehokkaita elinkeinoelämään kohdistuvia valvonta- ja seurantatoimia sekä velvoitteita tähän liittyen. Pelastakaa Lapset ry muistuttaa, että lapsilla on oikeus tulla kuulluksi itseään koskevissa päätöksissä ja suosittelee, että lapset osallistetaan mielekkäällä tavalla kyberturvallisuutta edistävän toiminnan suunnitteluun, harjoitteluun ja arviointiin.

Ulkoministeriön mielestä valtiotoimijoiden ja kansainvälisen yhteistyön merkitys Suomen kyberturvallisuuden kannalta ei tule riittävästi esille ohjelmassa. Ulkoministeriö katsookin, että suunnitelmassa tulisi nostaa paremmin esille kansalliseen turvallisuuteen liittyviä kysymyk-

siä ja toimeenpanossa tulisi keskittyä näihin haasteisiin, sekä keskittyä edistämään kansallista strategista ja operatiivista johtajuutta. Ulkoministeriö näkee myös, että Suomen kyberturvallisuusstrategian tulisi olla paremmin yhteensopiva EU:n kyberturvallisuusstrategian kanssa. Puolustusvoimat esittää puolestaan, että kyberturvallisuuden kehittämisohjelmassa tulisi huomioida Euroopan unionin kyberturvallisuusstrategian periaatteet nykyistä paremmin osana kansallisen kyberkyvykkyyden kehittämistä.

Valtioneuvoston kanslia haluaisi, että sen roolia ministeriöiden yhteisen tietoturvallisuuden ohjaajana ja yhteen sovittajana tuotaisiin paremmin esille ohjelmassa. Valtioneuvoston kanslia ehdottaa myös, että toimenpideohjelmaan lisättäisiin kyberturvallisuuteen liittyvien lainsäädäntötarpeiden kartoittamista. CSC-Tieteen tietotekniikan keskus Oy näkee hyödyllisenä lisätä ohjelmaan osuus kyberturvallisuuden tulevaisuudennäkymistä. CSC kiinnittää huomiota erityisesti kvanttiteknologian mukanaan tuomiin mahdollisuuksiin ja uhkiin, sekä niihin hyötyihin, joita uusiin teknologioihin panostaminen toisi mukanaan. Oikeusrekisterikeskus näkee perusteltuna ottaa ohjelmaan toimenpiteitä Post-quantum-algoritmien käytöstä. Suomen Kuntaliitto painottaa kuntien roolia kehittämistyön onnistumisen kannalta ja korostaa, että ohjelman tavoitteiden tulee olla toteutukseltaan yhteneviä tiedonhallintalain asettamien velvoitteiden kanssa. Kuntaliitto pitää tärkeänä periaatteena, että verkko- ja tietoturvaa koskevien uusien velvoitteiden ja vaatimusten tulee olla oikeasuhtaisia ja riskiperusteisia soveltamisalaan kuuluvien toimijoiden kokoon ja toimintaan nähden.

EK näkee tarpeelliseksi tarkastella ohjelman täytäntöönpanon riskejä. EK näkee tärkeänä, että kyberturvallisuutta tarkastellaan laajassa mittakaavassa, eikä näkökulmaa tulisi rajata pelkästään ohjelmassa nimenomaan mainittuihin kyberturvallisuushankkeisiin. EK pitää valtion tukea yrityksille viranomaisten valvontaresursseja tärkeämpänä. EK kiinnittää huomiota siihen, että turvallisuusselvityksien tulkintalinja on selvästi kaventunut aiemmasta siitä huolimatta, että lakia ei ole muutettu. Tietoturva ry kannattaa kansallisen tietoturvapäivän palauttamista. Huoltovarmuuskeskus HVK toivoo, että HVK:n Digitaalisen turvallisuuden 2030 -ohjelmasta käytetään hankkeen sijaan nimitystä ohjelma. HVK kiinnittää huomiota siihen, että ohjelmassa kyberturvallisuutta lähestytään hyvin teknologialähtöisesti, ja näkee, että tätä rajausta voitaisiin perustella enemmän. FiCom ry pitää kyberturvallisuuskeskuksen saamia lisäresursseja hyvänä asiana, sillä se mahdollistaa FiCom ry:n mielestä nopean reagoinnin poikkeustilanteisiin.

Wärtsilä painottaa kybermaailman globaalia luonnetta ja sen mukanaan tuomaa velvoitetta seurata kansainvälistä kehitystä. Wärtsilä pitää nykyistä sääntelykehystä puutteellisena sekä kansallisella, että kansainvälisellä tasolla, ja kiinnittää huomiota nykyisen markkinoilla vallitsevan ”first to market” periaatteen mukanaan tuomiin ongelmiin kyberturvallisuuden kannalta. Wärtsilä ehdottaa, että kokonaisvaltaisten kansainvälisten ja kansallisten toimintamallien kehittämiseen kohdennettaisiin resursseja. Wärtsilä näkee, että kansallista Centers of Excellence mallia ja metodeja voitaisiin hyödyntää monissa kehittämisohjelman teemoissa, kuten koulutuksessa, yhteistyössä ja tutkimus- ja kehitystyön edistämisessä. Wärtsilä lausuu, että se on erittäin sitoutunut parantamaan kansallista ja kansainvälistä kyberuhkiin liittyvää yhteistyötä sekä olemaan kokonaisvaltaisesti mukana turvallisemman digitaalisen tulevaisuuden rakentamisessa. Maanpuolustuskoulutusyhdistys näkee, että erityisesti kyberturvallisuuden puolella muun muassa kaluston ja tietoliikenneyhteyksien kustannusten rahoitukseen tulisi erikseen kiinnittää huomiota.

Puolustusvoimat painottaa, että muuttuneessa digitaalisessa toimintaympäristössä kyberpuolustuksella ja kansallisen turvallisuuden näkökulmien huomioimisella on aiempaa korostuneempi merkitys. Puolustusvoimat näkee, että kehittämisohjelman merkittävimmät puutteet ovat kansallisen turvallisuuden ja kyberpuolustuksen kehittämisessä. Puolustusvoimat korostaa myös, että tavoitteisiin, joiden keskeinen resurssi on vapaaehtoinen osallistuminen kunkin omilla resursseilla, liittyy merkittäviä riskejä toteutumisen kannalta. Puolustusvoimien mielestä kehittämisohjelman jäsentämiseksi tulisi harkita esimerkiksi vaiheistamista, vaihekohtaisia strategisia tavoitteita ja vaiheiden suunnittelun aikataulun kuvaamista. Lisäksi Puolustusvoimat näkee, että kehittämisohjelmassa tulisi esittää selvästi yhteys, miten esitetyillä toimenpidelistauksilla saavutetaan uskottavasti kaikki Suomen kyberturvallisuusstrategian tavoitteet. Puolustusvoimat esittää myös kehittämistoimenpiteiden lisäämistä kehittämisohjelmaan vuoden 2019 kyberturvallisuusstrategiassa olevan kybertoimintaympäristön suojaamistavoitteen saavuttamiseksi. Puolustusvoimat näkee, että kehittämisohjelman ekosysteemiä tulisi lähteä rakentamaan kansallisen tason kyberturvallisuuden ja kyberpuolustuksen kautta. Puolustusvoimat tuo myös esille, että ohjelma ei tällä hetkellä ole sellainen kokonaisvaltainen kansallisen kyberturvallisuusstrategian kehittämisohjelma, kuten kyberturvallisuusstrategioiden pohjilta voisi olettaa. Kehittämisohjelman tulisi Puolustusvoimien mukaan sisältää kansallisen turvallisuuden ja kyberpuolustuksen kriittisiä ja laajoja kehittämistarpeita. Puolustusvoimat esittää, että kehittämisohjelmaa kehitetään vastaamaan näitä tarpeita. Puolustusvoimat tuo myös esiin, että kyberturvallisuuden toimintaympäristön nopea muutos, sekä oman ymmärryksen lisääntyminen toimintaympäristöstä edellyttävät kyberturvallisuusstrategian ajantasaisuutta. Puolustusvoimat esittää, että seuraava kyberturvallisuusstrategiatyö aloitetaan viimeistään 2020-luvun puolivälissä.

CySec Ice Wall oy kiinnittää huomiota tietomurtoihin ja tuo esiin useita kehitystarpeita tietomurtojen tutkittavuus- ja todistettavuuskyvykkyyden edistämiseksi esimerkiksi organisaatioiden tietoverkkoihin, järjestelmien käyttäjien eriyttämiseen ja lainsäädännöllisiin muutoksiin liittyen. Erityisesti CySec Ice Wall oy korostaa kyberturvallisuuden kannalta vaarallisten työyhdistelmien poistamisen tärkeyttä, sekä verkkodatahistorian merkitystä tietomurtojen selvittämisen kannalta. Tietosuojavaltuutetun toimisto tuo esille, että ohjelmassa jää osin epäselväksi, mikä asema henkilötietojen suojalla on osana kyberturvallisuutta ja mikä on eri turvallisuuden osa-alueiden välinen suhde. Tietosuojavaltuutetun toimisto korostaa myös henkilötietoihin kohdistuvien tietoturvaloukkauksien merkitystä yhteiskunnan kannalta kriittisten toimialojen toimintaan ja yksittäisten henkilöiden arkeen. Yksityishenkilöiden taholta kiinnitetään huomiota rakennetun ympäristön merkitykseen kyberturvallisuuden kannalta, ja nähdään, että sen huomioiminen kyberturvallisuuden kehittämisohjelmassa olisi perusteltua.

Turun kaupunki kiinnittää huomiota käsitteiden määrittelyyn ja erityisesti termien kyberturvallisuus, tietoturva, tietosuoja, digiturva ja kyberturva merkitykseen. IKI ry kiinnittää huomiota nykyisen PKI-infrastruktuurin olemassaoloon ja sen laajempiin hyödyntämismahdollisuuksiin viestinnän kyberturvallisuuden tason nostamisessa erityisesti arkipäivän tilanteissa. IKI ry painottaa myös älykortti-tunnistautumisen etuja SMS-tunnistautumiseen nähden. Microsoft korostaa, että loppukäyttäjä on tietoturvan kannalta organisaation suurin riski. Microsoft tuo myös esiin pilvipalveluiden hyödyntämisen merkityksen yritysten kyberturvallisuuden parantamisessa. Microsoft näkee lisäksi riskiperusteiset ja lopputulokseen keskittyvät tietoturvavaatimukset olennaisina tietoturvan parantamisen kannalta ja painottaa tietoturvallisuuden ja kyberturvallisuuden tärkeyttä organisaatioiden toiminnassa.