Kyberturvallisuuden kehittämisohjelma

LIIKENNE- JA VIESTINTÄMINISTERIÖ

Liikenne- ja viestintäministeriön julkaisuja **2021:7**

lvm.fi

Liikenne- ja viestintäministeriön julkaisuja 2021:7

Kyberturvallisuuden kehittämisohjelma

Rauli Paananen

Liikenne- ja viestintäministeriö Helsinki 2021

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Liikenne- ja viestintäministeriö

ISBN pdf: 978-952-243-599-6
ISSN pdf: 1795-4045

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2021

Kuvailulehti
10.6.2021

Kyberturvallisuuden kehittämisohjelma

Liikenne- ja viestintäministeriön julkaisuja 2021:7
Julkaisija Liikenne- ja viestintäministeriö

Tekijä/t Rauli Paananen
Kieli suomi **Sivumäärä** 44

Tiivistelmä

Kyberturvallisuuden kehittämisohjelma periaatepäätöksessä määritetään keskeiset toimenpiteet kyberturvallisuuden parantamiseksi koko yhteiskunnassa. Kyberturvallisuuden kehittämisohjelma lähestyy kansallista kyberturvallisuutta mahdollisuuksien näkökulmasta. Toteutuessaan eri toimenpiteet vahvistavat merkittävästi kansallista kyberturvallisuutta. Kehittämisohjelman ensisijaisena tavoitteena on luoda Suomeen kyberturvallisuuden ekosysteemi, joka tuottaa elinvoimaa ja kasvua, lisää alan työpaikkoja, luo tarvittavaa osaamista ja parantaa digitaalisen yhteiskunnan kestävyyttä sekä sietokykyä kybertoimintaympäristön eri ilmiöitä vastaan.

Vahva kansallinen kyberturvallisuus edellyttää tarvittavaa osaamista ja laajaa osallistumista yhteiskunnan kaikilla eri tasoilla, tiivistä yhteistyötä erityisesti julkishallinnon ja elinkeinoelämän välillä, vahvaa kotimaista kyberturvateollisuutta joka luo kyvykkyyksiä digitaalisen yhteiskunnan palveluiden turvaamiselle ja viranomaisten kyberturvakyvykkyyksiä jotka luovat pohjaa koko yhteiskunnan turvalliselle toiminnalle.

Periaatepäätös ja sen linjauksia edistävä toimeenpanosuunnitelma valmisteltiin liikenne- ja viestintäministeriön johdolla laajassa yhteistyössä yli 80 organisaation edustajien kanssa. Kehittämisohjelma on osa Suomen kyberturvallisuusstrategian 2019 ja EU:n kyberturvallisuusstrategian toimeenpanoa.

Asiasanat tietoturva, kyberturvallisuus, riskienhallinta, digitalisaatio

ISBN PDF 978-952-243-599-6 **ISSN PDF** 1795-4045
Asianumero VN/797/2021

Julkaisun osoite http://urn.fi/URN:ISBN:978-952-243-599-6

Presentationsblad
10.6.2021

Utvecklingsprogram för cybersäkerheten

Kommunikationsministeriets publikationer 2021:7
Utgivare Kommunikationsministeriet

Författare Rauli Paananen
Språk finska
Sidantal 44

Referat

I principbeslutet om utveckling av cybersäkerheten fastställs centrala åtgärder för att förbättra cybersäkerheten i hela samhället. Utvecklingsprogrammet för cybersäkerheten närmar sig den nationella cybersäkerheten med möjligheterna som utgångspunkt. När de olika åtgärderna förverkligas stärker de den nationella cybersäkerheten och livskraften, samtidigt som de minskar de cybersäkerhetsrisker som följer av de nuvarande bristerna eller flaskhalsarna. Det primära målet för utvecklingsprogrammet är att i Finland skapa ett cybersäkerhetsekosystem som genererar livskraft och tillväxt, ökar antalet arbetsplatser inom branschen, skapar den nödvändiga kompetensen och förbättrar det digitala samhällets hållbarhet och tålighet i förhållande till olika fenomen i cybermiljön.

Stark nationell cybersäkerhet förutsätter nödvändig kompetens och omfattande deltagande på alla olika nivåer av samhället, nära samarbete mellan i synnerhet den offentliga förvaltningen och näringslivet, en stark inhemsk cybersäkerhetsindustri som skapar kapaciteter att trygga tjänsterna i det digitala samhället och cybersäkerhetskapaciteter hos myndigheterna som lägger grunden för säker verksamhet i hela samhället.

Principbeslutet och genomförandeplanen som främjar riktlinjerna i detta bereddes under ledning av Kommunikationsministeriet i ett omfattande samarbete med representanter för över 80 organisationer. Utvecklingsprogrammet är en del av verkställandet av Finlands cybersäkerhetsstrategi 2019 och EU:s cybersäkerhetsstrategi.

Nyckelord datasäkerhet, cybersäkerhet, digitalisering, riskhantering

ISBN PDF 978-952-243-599-6
ISSN PDF 1795-4045
Ärendenummer VN/797/2021

URN-adress http://urn.fi/URN:ISBN:978-952-243-599-6

Description sheet
10 June 2021

Cyber Security Development Programme

Publications of the Ministry of Transport and Communications 2021:7
Publisher Ministry of Transport and Communications

Authors Rauli Paananen
Language Finnish **Pages** 44

Abstract

The resolution on the Cyber Security Development Programme defines the key measures to improve cyber security throughout society. The approach in the Programme towards national cyber security is through opportunities. When implemented, the measures will significantly strengthen national cyber security. The primary aim of the Programme is to create a cyber security ecosystem in Finland that will provide vitality and growth, create jobs in the sector, increase necessary expertise and improve both the sustainability of the digital society and its resilience to the different phenomena in the cyber security environment.

High-level, national cyber security calls for necessary expertise, extensive participation across all levels of society, close cooperation between the public administration and business life, strong domestic cyber security industry that will provide potential for ensuring the services in digital society, and the authorities' cyber security capabilities that will form the basis for secure operation of the entire society.

The resolution and the action plan promoting its policies were prepared under the leadership of the Ministry of Transport and Communications and in cooperation with representatives from more than 80 organisations. The Development Programme is part of the implementation of the Finnish Cyber Security Strategy 2019 and the EU Cyber Security Strategy.

Keywords information security, cyber security, risk management, digitalisation

ISBN PDF 978-952-243-599-6 **ISSN PDF** 1795-4045
Reference number VN/797/2021

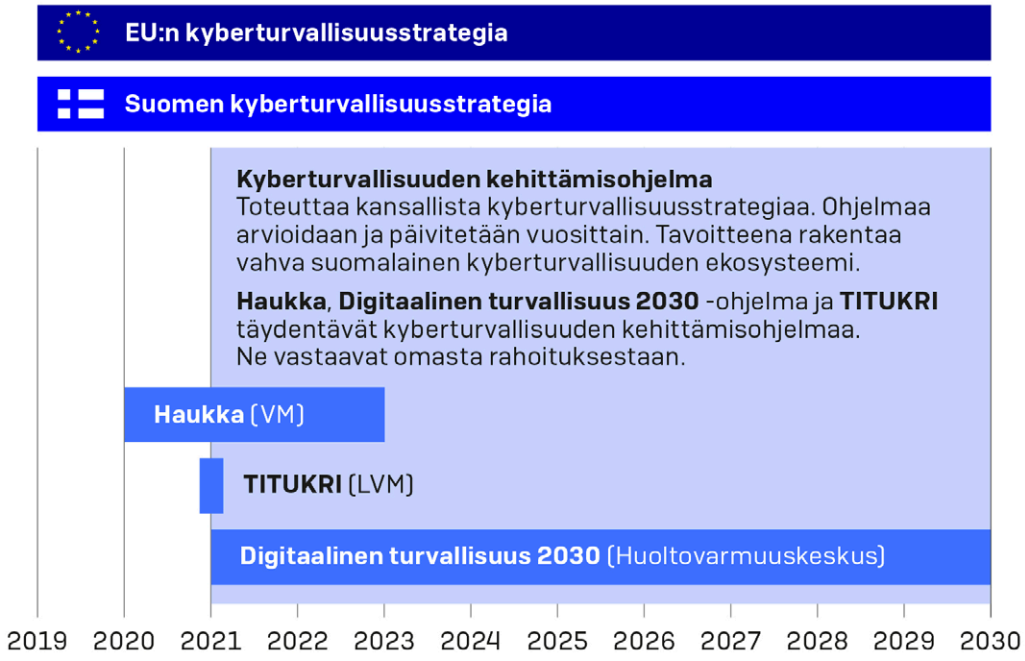
URN address http://urn.fi/URN:ISBN:978-952-243-599-6

Sisältö

1 Johdanto

Pääministeri Sanna Marinin hallitusohjelmassa on asetettu tavoitteita kansallisen kyberturvallisuuden kehittämisestä liittyen tilannekuvan parantamiseen, kansainvälisen yhteistyön tiivistämiseen sekä kansallisen koordinaation tehostamiseen. Vuonna 2019 annetussa valtioneuvoston periaatepäätöksessä Suomen kyberturvallisuusstrategiasta on tunnistettu tarve kansallisen kyberturvallisuuden kokonaistilan parantamiseksi. Kyberturvallisuusstrategia on osa yhteiskunnan turvallisuusstrategian (2017) ja EU:n kyberturvallisuusstrategian toimeenpanoa. Tämä periaatepäätös kansallisen kyberturvallisuuden kehittämisestä vastaa edellä mainittuihin tavoitteisiin.

Kuva 1. Kyberturvallisuuden kehittämisohjelma ja sen keskeiset osat



Haukka: Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023. Ohjelmassa kehitetään julkisen hallinnon digitaalisen turvallisuuden palveluita.

TITUKRI: Raportti lainsäädännön muutostarpeista ja muista toimenpiteistä tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla.

Digitaalinen turvallisuus 2030: Ohjelman tehtävänä on yhteiskunnan digitaalisen infrastruktuurin ja sen palvelujen häiriönsiedon ja kyberturvallisuuden kehittäminen.

Tietoturvallisuuden ja tietosuojan parantaminen kriittisillä toimialoilla -työryhmän (TI-TUKRI) loppuraportissa esittämät toimenpide-ehdotukset ovat yhteiskunnan kannalta merkittäviä ja tukevat kyberturvallisuuden kehittämisohjelmassa esitettyjä toimenpiteitä. Valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta ja sen toimeenpanosuunnitelma sekä Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -ohjelma täydentävät tätä periaatepäätöstä ja vastaavat omasta rahoituksestaan. Kokonaisuutena kyse on erittäin laaja-alaisesta ja kattavasta yhteiskunnan kyberturvallisuuden kehittämiseen tähtäävästä toimenpidekokonaisuudesta (kuva 1).

Kyberturvallisuuden kokonaistilan parantamista koskevaan tarpeeseen ovat vaikuttaneet yhteiskunnan toimintaympäristössä tapahtuneet merkittävät muutokset, jatkuvasti kehittyvät kyberturvallisuusuhkat, ICT-ympäristöjen kompleksisuuden lisääntyminen, sulautettujen ja perinteisten ICT-järjestelmien konvergenssi sekä kansallisessa toiminnassa havaitut kehittämiskohteet. Kyberturvallisuusuhkien realisoitumisen nähdään aiheuttavan myös entistä suurempia vaikutuksia vahvasti verkottuneen yhteiskunnan kriittisille toiminnoille ja tietosuojalle. Yhteiskunta on yhä riippuvaisempi digitaalisesta toimintaympäristöstä, minkä vuoksi kyberturvallisuuden tulee olla sisäänrakennettuna kaikessa toiminnassa, prosesseissa ja järjestelmissä, joihin kohdistuu uhkatekijöitä. Hyvä kyberturvallisuuden taso voidaan saavuttaa vain, jos jokainen digitaaliseen yhteiskuntaan kytkeytynyt toimija kantaa oman vastuunsa kyberturvallisuuden toteutumisesta. Kyberturvallisuus tulee nähdä luonnollisena osana jokaisen organisaation ja yksilöiden yhteiskuntavastuuta.

Kehittämisohjelman aikajänne on 2021–2030 ja se kuvaa kyberturvallisuuden kehittämisen lyhyen ja pitkän aikavälin tavoitteita ja painopistealueita. Kehittämisohjelman toimeenpanosuunnitelma kuvaa puolestaan tavoitteiden saavuttamiseksi tarvittavat toimenpiteet vastuineen ja mittareineen. Kehittämisohjelman toimenpiteiden vaikuttavuutta on arvioitu kansainvälisestä, kansallisesta, hallinnon- ja toimialan, yrityksen sekä kansalaisen näkökulmasta huomioiden nyky- ja tavoitetila sekä soveltuvin osin tarvittavat investoinnit. Toimeenpanosuunnitelman ajantasaisuutta arvioidaan ja toimenpiteitä päivitetään vuosittain. Kehittämisohjelman toteuttaminen edellyttää 5,9 miljoonan euron rahoitusta vuosittain ajanjaksolle 2022–2025. Kehittämisohjelman rahoituksesta päätetään julkisen talouden suunnitelman ja valtion talousarvion valmistelun yhteydessä. Toimenpiteiden mahdollisesti edellyttämä valtion rahoitus toteutetaan valtiontalouden kehysten puitteissa tarvittaessa kohdentamalla määrärahoja uudelleen.

Kyberturvallisuuden kehittämisohjelman toteutusta sekä kehittämistoimien ajantasaisuutta seurataan säännöllisesti liikenne- ja viestintäministeriössä sekä Turvallisuuskomiteassa. Kehittämisohjelman toimeenpano käynnistetään välittömästi.

Kehittämisohjelman toteuttamista tukee kyberturvallisuusstrategiassa asetettu kyberturvallisuuden johtamisen koordinaatiomalli. Koordinaatiomallissa huomioidaan julkisen hallinnon ja elinkeinoelämän kyberturvallisuuden suunnittelu, kehittäminen ja yhteistyö. Liikenne- ja viestintäministeriöön sijoitetun kyberturvallisuusjohtajan tehtävänä on kehittää kybertoimintaympäristön yhteistyötä ja osaamista eri sektoreilla. Näiden lisäksi, osana tätä kehittämisohjelmaa, parannetaan laajojen kyberturvallisuushäiriöiden operatiivisen tilannekuvan muodostamista ja operatiivista johtamista. Lisäksi huomioidaan kansainvälinen toimintaympäristö sekä kansainvälisen tason prosessit ja käytänteet, joilla pyritään parantamaan kyberturvallisuutta muun muassa EU:n piirissä.

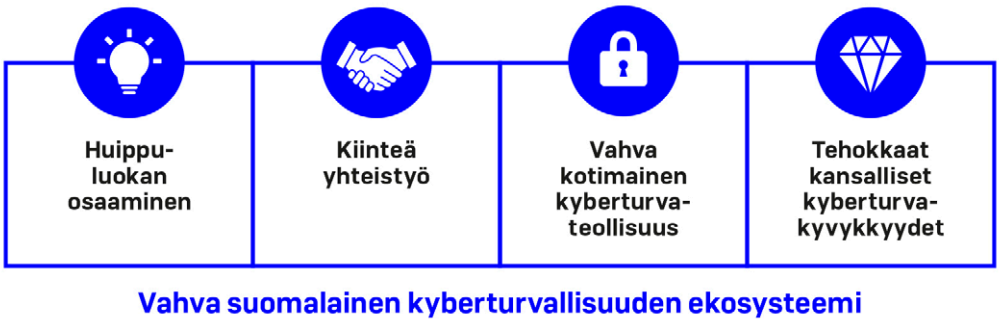
Kehittämisohjelman valmisteluun osallistui yli 80 eri organisaatiota. Kehittämisohjelman valmistelun yhteydessä järjestettyihin työpajoihin osallistuivat muun muassa elinkeinoelämä, kyberturvateollisuus, valtionhallinto, yliopistoja sekä eri järjestöjä.

2 Kehittämisohjelman tavoite ja pääteemat

Kyberturvallisuuden kehittämisohjelma lähestyy kansallista kyberturvallisuutta ennen kaikkea mahdollisuuksien näkökulmasta, jotka toteutuessaan vahvistavat kansallista kyberturvallisuutta ja elinvoimaa, pienentäen samalla nykyisistä puutteista tai kapeikoista johtuvia kyberturvariskejä. **Kehittämisohjelman ensisijaisena tavoitteena on luoda Suomeen kyberturvallisuuden ekosysteemi** (kuva 2), joka tuottaa elinvoimaa ja kasvua, lisää alan työpaikkoja, luo tarvittavaa osaamista ja parantaa digitaalisen yhteiskunnan kestävyyttä sekä sietokykyä kybertoimintaympäristön eri ilmiöitä vastaan.

Kehittämisohjelma pureutuu ensin neljään ekosysteemin kasvattamisen näkökulmasta keskeiseen pääteemaan. Nämä neljä teemaa ovat: **huippuluokan osaaminen**, **kiinteä yhteistyö**, **vahva kotimainen kyberturvateollisuus** ja **tehokkaat kansalliset kyberturvakyvykkyydet**. Kehittämisohjelman tulevien päivityskierroksien yhteydessä voidaan ottaa mukaan myös uusia teemoja.

Kuva 2. Suomalaisen kyberturvallisuuden ekosysteemi



3 Huippuluokan osaaminen

Vahva kansallinen kyberturvallisuus edellyttää tarvittavaa osaamista ja laajaa osallistumista yhteiskunnan kaikilla eri tasoilla. Digitaalisten ratkaisujen ja palveluiden tarjoajien on kyettävä tuottamaan turvallisia palveluita. Kansalaisten on osattava puolestaan käyttää digitaalisen tietoyhteiskunnan tuottamia palveluita turvallisesti ja tunnistettava eri laitteiden, tuotteiden ja palveluiden käyttöön liittyvät riskit. Kansalaisten osaamisen kasvattamisessa korostuu kolmannen sektorin ja vapaan sivistystyön rooli. Yhteiskunnan on vastattava omalta osaltaan tähän tarpeeseen luottamuksen kasvattamisen mahdollistamiseksi.

Suomalainen elinkeinoelämä, kyberturvateollisuus ja viranomaiset ovat tuoneet esille kyberturva-osaajien määrän riittämättömyyden nyt ja tulevina vuosina. Kyberturvallisuuden huippuosaajista käydään jatkuvasti kovaa kansainvälistä kilpailua. Kansainväliset osaajat ovat usein edellytys alan yritysten kasvulle, kansainvälistymiselle ja uusille innovaatioille. Huippuosaajat ovat myös vetovoimatekijä, joka houkuttelee muitakin erityisosaajia. Huippuosaajia tarvitaan edistämään suomalaisen kyberturvallisuusteollisuuden, elinkeinoelämän ja tutkimuksen menestymistä globaaleilla markkinoilla.

Nykyiset koulutusohjelmat eivät suoraan tuota tarvittavaa osaamista suomalaiselle kyberturvateollisuudelle, elinkeinoelämälle ja viranomaisille. Tämä johtaa tilanteeseen, jossa eri tahot joutuvat myös kilpailemaan jatkuvasti samoista osaajista, sekä jatkokouluttamaan uutta henkilöstöään merkittävästi työtehtävien aloittamisen yhteydessä. Parhaimman vaikuttavuuden varmistamiseksi kyberturvallisuuden koulutusohjelman tuottamat tutkinto-opinnot tulee suunnitella yhteistyössä eri toimijoiden kanssa ja opintojen sisältöjä tulee päivittää säännöllisesti vastaamaan eri toimijoiden tarpeita. Edelleen kyberturvallisuuden opetuksen pitäisi olla sisällytettynä niissä tutkinto-opinnoissa, joissa luodaan osaamista teknologia-aloille. Tämä edistää turvallisuuden toteuttamista sisäänrakennettuna yhteiskunnan eri infrastruktuureihin, toimintoihin ja palveluihin. Osaamisvajeen paikkaamiseksi ja riittävän laaja-alaisen ja monipuolisen osaamisen varmistamiseksi tulee naisia ja tyttöjä sekä muita aliedustettuja ryhmiä kannustaa ja rohkaista kyberalalle.

Kyberturvallisuuden ammatillisen osaamisen edistämiseksi tarvitaan panostuksia tutkintoon johtavaan koulutukseen sekä muunto-, että täydennyskoulutukseen kyberturvaosaajien kasvattamiseksi julkiselle ja yksityiselle sektorille. Lisäksi yliopisto- ja ammattikorkeakoulutuksessa tulee lisätä kyberturvallisuuden sivuainekoulutusta erillisenä opintokokonaisuutena, jotta kyberturvallisuusopintoja voidaan tarjota muillekin kuin kyberturvallisuusalan opiskelijoille. Kehitysohjelma kannustaa myös työnantajien ja oppilaitosten yhä tiiviimpään yhteistyöhön esimerkiksi työharjoittelujaksojen lisäämisessä. Tämä helpottaa alan opintojen soveltamista työelämässä sekä edistää varsinaista työelämään siirtymistä.

Kansainvälisesti kilpailukykyisten ja turvallisten kyberturvatuotteiden ja -palveluiden kehittäminen edellyttää, että yrityksillä on käytettävissään kyberturvateknologian ja -prosessien huippuosaajia, jotka hallitsevat syvällisesti alan keskeiset osa-alueet. Kansallisen kyberturvallisuuden huippuosaamisen kehittäminen edellyttää riittävän osaamiskeskittymän muodostumista. Huippuosaamiskeskittymän muodostaminen edellyttää puolestaan korkeakoulujen välistä tiivistä yhteistyötä kansallisesti ja kansainvälisesti, monitieteellisyyttä ja usean muun eri sidosryhmän yhteistyötä. Kehittämiseen tulee sitouttaa mukaan opetus- ja koulutusalan toimijat (peruskoulut, lukiot, ammattikoulut, ammattikorkeakoulut, yliopistot), tutkimuslaitokset, julkishallinto, elinkeinoelämän keskeiset toimijat ja yhteistyöekosysteemit, yhteiskunnan kriittiseen infrastruktuuriin liittyvät toimijat sekä kyberturva-alan yritykset ja toimijat. Lisäksi tulee kannustaa vahvistamaan ja syventämään kansainvälistä yhteistyötä ja luoda tiiviitä suhteita kansainvälisiin huippuosaamiskeskittymiin.

3.1 Ehdotetut kehittämistoimenpiteet

Kansalaisten kyberturvataidot hyvälle tasolle

Järjestöjen ja vapaaehtoisten yhteisöjen roolia vahvistetaan kansalaisten kyberturvataitojen kehittämisessä. Järjestöjen rooli määritellään kansalaisten kyberturvallisuuden turvallisuusviestintätyössä ja niiden toimintaa tuetaan tässä tehtävässä.

Kansalaisten tietoisuuden kasvattamista tehostetaan edelleen osana Euroopan kyberturvakuukautta sekä Digi- ja väestötietoviraston koordinoimaa kansallista digiturvaviikkoa, jonka osaksi palautetaan myös kansallinen tietoturvapäivä. Vapaaehtoisuuteen perustuvien kyberturvayhteisöjen toimintaa tuetaan ja osaamista hyödynnetään sekä yleisen että syventävän osaamisen kehittämisessä.

Edelleen järjestöjä tuetaan myös vakavien kyberhyökkäystilanteiden jälkihoitoon liittyvissä valmiuksissa sekä näiden toteutuksessa yhteistyössä viranomaisten kanssa. Tämä edellyttää vastuu- ja toimintamallien päivittämistä, sekä jälkihoitoa tarjoavien toimijoiden osaamisen kasvattamista kyberhyökkäyksien vaikutuksista ja niiden seurauksista.

Edellä olevien lisäksi luodaan viestintäsuunnitelma tarvittavine toimenpiteineen kansalaisten kyberturvallisuustietoisuuden kasvattamiseksi.

Kyberturvallisuuden koulutuksen kehittäminen

Kyberturvallisuuden koulutuksen suunnittelussa pyritään huomioimaan sekä elinkeinoelämän, että julkishallinnon kyberturvallisuuden osaamistarpeet. Mahdollisuuksien mukaan varhaiskasvatuksessa pyritään luomaan lapsille perusteet ymmärtää, kuinka digitaalisen yhteiskunnan tuotteita ja palveluita käytetään turvallisesti. Kyberturvallisuuden sisällyttämistä peruskoulun opetussuunnitelmiin harkitaan erillisen tutkimuksen pohjalta. Yleissivistävässä perusopetuksessa pyritään varmistamaan, että nuorilla olisi riittävät taidot toimia digitaalisessa toimintaympäristössä ja he ymmärtäisivät kyberturvauhkat sekä osaisivat suojautua niiltä.

Lukiokoulutuksessa pyritään mahdollisuuksien mukaan laajentamaan ja syventämään näitä taitoja ja luodaan perustaa alan erityisosaamiselle korkea-asteen koulutuksessa. Ammatilliseen koulutukseen pyritään soveltuvin osin sisällyttämään kyberturva-asiat osaksi alan perusammattitaitoa. Turvallinen toimiminen digitaalisessa ympäristössä ja siihen liittyvä osaaminen pyritään integroimaan opiskeluun ammattialaan soveltuvalla tavalla, opiskeltavasta ja ammatista riippumatta. Ammatillisen ja täydentävän kyberturvaosaamisen kehittämiseksi pyritään suunnittelemaan osaamispolkuja, joissa hyödynnetään jo olemassa olevia sisältöjä ja luodaan tarvittaessa uusia. Kannustetaan naisia ja tyttöjä sekä muita aliedustettuja ryhmiä kiinnostumaan kyberalasta.

Huippu- ja erityisosaamistarpeet tunnistetaan ja osaamista kehitetään tarpeiden mukaisesti. Yhteisiä kyberturvakoulutuksia järjestetään keskitetysti toimialasta riippumatta. Tuetaan kansainvälisten huippukoulutusten ja -kouluttajien tuomista Suomeen ja luodaan suhteita kansainvälisiin huippuosaamiskeskittymiin. Koulutusten järjestämisessä hyödynnetään mahdollisuuksien mukaan virtuaalitoteutuksia sekä muita kustannustehokkaita ratkaisuja.

4 Kiinteä yhteistyö

Yhdeksi merkittäväksi mahdollisuudeksi on tunnistettu yhteistyön edelleen tiivistäminen erityisesti julkishallinnon sekä elinkeinoelämän välillä. Tämä nähdään merkittävänä tekijänä kyberturvallisuuden ekosysteemin vahvistamisessa. Kansallisen kyberturvakentän toimijoiden yhteistyölle halutaan löytää uusia tapoja ja yhteistyön muotoja. Kyberturvayhteisöjä halutaan aktivoida myös enemmän valtionhallinnon digitaalisten palveluiden kyberturvallisuuden jatkuvaan parantamiseen.

Kyberturvallisuuden harjoitustoimintaa ylläpidetään ja edistetään. Aktiivisella harjoitustoiminnalla on keskeinen merkitys kyberhyökkäyksien torjunnan, hallinnan ja niiden ratkaisemisen kehittämisessä. Yhteistyössä toimiminen Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelman 2020–2023 (Haukka) sekä Digitaalinen turvallisuus 2030 -hankkeen kanssa on keskeistä näiden kyvykkyyksien edistämiseksi.

Kehittämisohjelma kannustaa strategisten kumppanuusmallien lisäämiseen yritysten ja yliopistojen sekä korkeakoulujen välillä. Pitkäjänteisen yhteistyön tulisi mahdollistaa tutkimus- ja kehittämistyön kautta uusien tuote- ja palveluinnovaatioiden syntyminen. Tämä edistää kotimaisen kyberturvateollisuuden tuotteiden ja ratkaisujen kaupallistamista.

Aktiivinen kansainvälinen yhteistyö luo osaltaan edellytyksiä kyberturvallisuuden ekosysteemin kasvulle ja turvallisen digitaalisen yhteiskunnan ylläpitämiselle sekä kehittämiselle ja laajemmin Suomen turvallisuuden vahvistamiselle. Kansainvälinen yhteistyö nähdään keskeisenä mahdollisuutena turvallisen Suomi-kuvan edistämiselle ja yhteensopivien kyberturvallisuuden viitekehysten rakentamiselle. Kyberturvallisuuden viitekehysten kansainvälinen yhteensopivuus on usein myös kasvun elinehto. Yhteistyö mahdollistaa kansainvälisen kyberturvallisuustason vertailun, joka tukee turvallisen digitaalisen yhteiskunnan edistämistä ja jatkuvan parantamisen kehityspolkua.

4.1 Ehdotetut kehittämistoimenpiteet

Kyberturvallisuuden harjoitustoiminnan yhteistyön vahvistaminen

Tehdään tiivistä yhteistyötä kyberturvallisuuden harjoitustoiminnassa viranomaisten, elinkeinoelämän ja järjestöjen välillä yhteiskunnan toimivuuden kannalta kriittisten arvoketjujen toiminnan turvaamiseksi. Kyberturvallisuuden harjoitustoiminnassa hyödynnetään yhteisiä kyberharjoitusympäristöjä. Varmistetaan harjoitustoiminnan jatkuminen ja näiden poikkihallinnollinen ohjaus. Lisäksi tuetaan EU:n kyberturvallisuuteen ja uhkiin liittyvien harjoitusten järjestämistä.

Kansallisen kyberturvallisuuden tutkimus- ja kehittämisyhteistyön edistäminen

Kyberturvallisuuden tutkimus- ja kehittämisyhteistyötä koordinoidaan yhteisten tavoitteiden saavuttamiseksi. Kyberturvatutkimuksen kotimaisen ja kansainvälisen rahoituksen saatavuutta edistetään, turvallisuusnäkökohdat huomioiden. Teoreettisten tutkimustuloksien lisäksi tunnistetaan entistä enemmän mahdollisuuksia tulosten kaupallistamiseen ja tuetaan näiden edistämistä. Tutkimustoiminta otetaan osaksi yritysten innovaatio-, tuote- ja palvelukehitysprosesseja sekä kansainvälistä yhteistyötä.

Kyberturvayhteisöä aktivoidaan entistä laajemmin valtionhallinnon digitaalisten palveluiden turvallisuuden varmistamiseen. Yhteisön osaamista voidaan hyödyntää esimerkiksi turvallisen ohjelmistokoodin kehittämisessä ja käynnistämällä soveltuvin osin valtionhallinnon ”Bug Bounty” –ohjelmia, digitaalisten palveluiden turvallisuuden jatkuvaksi parantamiseksi.

Aktiivinen osallistuminen ja vaikuttaminen kansalliseen ja kansainväliseen kyberturvallisuuden yhteistyöhön

Suomi osallistuu ja vaikuttaa aktiivisesti EU:n kyberturvallisuuteen liittyvän yhteisen ulko- ja turvallisuuspolitiikan kehittämiseen ja tekee yhteistyötä EU:n kybertoimintakyvyn vahvistamiseksi. Tavoitteena on vapaa, avoin ja turvallinen kybertoimintaympäristö, jossa demokratiaperiaatetta, ihmisoikeuksia ja kansainvälistä lakia kunnioitetaan. Operationaalisella tasolla muun muassa verkko- ja tietoturva-asioista vastaavien (NIS) viranomaisten, lainvalvonta- ja oikeusviranomaisten sekä kyberdiplomatiasta ja kyberpuolustuksesta vastaavien toimijoiden välisen yhteistyön ja yhteistoiminnan vahvistaminen jäsenmaissa ja EU-tasolla on kannatettavaa. Lisäksi osallistutaan aktiivisesti kansainväliseen kyberturvayhteistyöhön keskeisissä kansainvälisissä järjestöissä (mm. YK, OECD, ETYJ, ITU-T ja Nato-kumppanuuden puitteissa) sekä bilateraaliyhteistyöhön.

Työn tavoitteena on suomalaisen kyberturvaosaamisen tunnettuuden kasvattaminen, yhteisten kyberturvavaatimusten, standardien sekä sertifiointiarviointikriteeristöjen valmistelu, tiedonvaihto ja yhteisen suomalaisen kyberturva-agendan edistäminen osana globaalia toimintaympäristöä. Kyberturvateollisuuden osallistumista edellä mainittujen kansainvälisten yhteistyöryhmien kannan muodostamiseen tuetaan perustamalla teema-aiheisia yhteistyöryhmiä. Lisäksi suomalaisten toimijoiden tulee kyetä tehokkaasti vaikuttamaan kansainvälisiin prosesseihin ja käytäntöihin, joiden kautta Suomen kyberturvallisuutta parannetaan.

Suomen menestymistä kansainvälisellä kyberturvakentällä seurataan kansainvälisiin indekseihin perustuen (ITU: Global Cybersecurity Index (GCI) ja e-Governance Academy: National Cyber Security Index (NCSI).

5 Vahva kotimainen kyberturvateollisuus

Vahva kotimainen kyberturvateollisuus on yksi kansallisen kyberturvallisuuden ekosysteemin keskeisimmistä mahdollistajista. Kyberturvateollisuus luo kyvykkyyksiä digitaalisen tietoyhteiskunnan palveluiden turvaamiselle, taloudelliselle kasvulle, osaamisen kasvattamiselle sekä uusille työpaikoille. Vahvan kotimaisen kyberturvateollisuuden kasvamisen edellytykset ovat riippuvaisia tämän kehittämisohjelman muista pääteemoista. Suomi tarvitsee lisää menestyviä kyberturvallisuustuotteita ja -palveluita, uusia kyberturvayrityksiä, olemassa olevien yrityksien kasvun ja kansainvälistymisen tukea sekä eri toimijoiden välistä yhteistyötä. Vahva kyberturvateollisuus luo myös pohjan kansallisen kyberturvallisuuden ekosysteemin omavaraisuuden tavoittelulle.

Kasvavat kansainväliset kyberturvallisuusmarkkinat ovat Suomelle merkittävä mahdollisuus talouskasvun ja työllisyyden näkökulmasta. Suomen tulee olla kansainvälisesti houkutteleva kyberturvallisuus-, ICT-alan liiketoiminta- ja investointiympäristö. Kansainvälisten yritysten sijoittuminen Suomeen, tutkimus- ja tuotekehityspanostukset Suomessa ja toimiva yhteistyö suomalaisten toimijoiden kanssa ovat keskeinen osa kyberturvallisuusalan ekosysteemin syntyä sekä kansallisen ja kansainvälisen kyberturvallisuusmarkkinan kasvua.

Vahvan kotimaisen kyberturvateollisuuden kehittäminen edellyttää useita teknologisia ja kaupallisia kyvykkyyksiä, joiden edistäminen huomioidaan osana kehittämisohjelmaa. Uusien yritysten perustamisen tukeminen, uuden kotimaisen IPR:n (kuten esim. immateriaalioikeudet teknologioissa sekä ohjelmistotuotteissa) syntyminen, tarvittavan osaamisen synnyttäminen ja tukeminen, erilaisten roolien tunnistaminen sekä hyödyntäminen kansainvälisessä ekosysteemissä ovat tärkeitä osatekijöitä kaupallisten kyvykkyyksien rakentamisessa. Uusista kansallisista innovaatioista, tuotteista ja palveluista on haettava kasvua myös kansainvälisesti.

Vuonna 2021 perustettava EU:n kyberturvallisuuden kompetenssikeskus ja sen yhteyspisteeksi ja verkoston osaksi Suomeen nimettävä kansallinen koordinaatiokeskus tulevat rahoittamaan kyberturvallisuuden tutkimushankkeita ja kyberturvallisuuden kompetenssien kehittämistä, kohderyhmänä erityisesti pk-yritykset. Kansallisella koordinaatiokeskuksella tulee olla kyberturvallisuuden substanssiosaamista, sekä kyky auttaa kokoamaan yhteen tutkimushankkeita ja tukea yrityksiä kehittämään kotimaisia tuotteita ja palveluita, jotka edelleen edistävät kansallisen kyberturvallisuuden ekosysteemin rakentumista sekä vientiä.

5.1 Ehdotetut kehittämistoimenpiteet

Kotimaisten kyberturvatuotteiden ja -palveluiden kasvun ja kansainvälistymisen tukeminen

Vahvan kotimaisen kyberteollisuuden kehittäminen vaatii kasvua, kansainvälistymistä sekä investointeja. Laaditaan tämän perustaksi kyberturvallisuusalan kasvustrategia, jolla tuetaan markkinoiden kasvua sekä edistetään Suomeen tehtävien kansainvälisten investointien saatavuutta, jotka luovat pohjaa myös kansallisen ekosysteemin kehittymiselle.

Kotimaisen kyberturvateollisuuden innovaatioita, tuotteita ja ratkaisuita hyödynnetään entistä laajemmin ja rohkeammin. Kehitetään hankintaosaamista kyberturvallisuuden tuotteiden ja palveluiden ostoon. Nähdään kokeilevan kulttuurin mahdollisuudet ja tuetaan kokeiluja sekä näiden kaupallistamista. Yhteensovitetaan edellä mainittuja tavoitteita yhteen Kansallisen julkisten hankintojen strategian 2020 toimenpiteiden kanssa.

Aktivoidaan Suomen ulkomaanedustustoja ja erityisesti niiden yhteydessä toimivaa Business Finland -verkostoa entistä enemmän kansainväliseen yhteistyöhön suomalaisen kyberturvaosaamisen tunnettuuden edistämiseksi. Kehitetään kansallista tiedonvaihtoa, jotta Suomen kyberturvaetuja ja edunvalvontaa voidaan ajaa hajautetusti, mutta yhtenä rintamana ja yhtenäisellä viestillä eteenpäin.

Edistetään tuotteiden ja palveluiden tuotteistamista ja konseptointia kansainvälisen markkinan näkökulmasta. Hyödynnetään Suomen vahvuuksia kansainvälistymisessä ja markkinoinnissa. Tuetaan myös Suomeen tehtävien kansainvälisten investointien saatavuutta, mikä luo pohjaa kansallisen ekosysteemin kehittymiselle.

Uusien kyberturvayritysten perustamisen edistäminen

Vahva kotimainen kyberturvateollisuus vaatii toteutuakseen eri elinkaaren vaiheissa olevia kyberturvayrityksiä. Jotta tämä olisi mahdollista, tulee eri elinkaaren vaiheissa olevien kyberturvayritysten kehittymistä tukea sekä niiden syntyä ja kasvua mahdollistaa. Yritykset tarvitsevat kyberturvateollisuudelle relevanttien kotimaisten rahoitusinstrumenttien sekä pääomien saatavuuden parantamista mukaan lukien mahdolliset valtion rahoitus- ja omistusosuudet.

Vahvistetaan erityisesti pk-yritysten kyberturvallisuusosaamisen tukirakenteita vuonna 2021 valittavien EU-rahoitteisten kansallisten keskittymien ja verkostojen avulla. Tässä työssä hyödynnetään EU:n kompetenssikeskuksen ja kansallisen koordinaatiokeskuksen toimintaa kyberturvayritysten perustamisen edistämisessä perustamalla kyberturvallisuuden kasvu- ja osaamiskeskus kansallisen koordinaatiokeskuksen yhteyteen. Jatketaan ja edelleen tiivistetään yhteistyötä mm. työ- ja elinkeinoministeriön, Business Finlandin, Kyberalan (FISC) sekä muiden tarvittavien yhteistyötahojen kanssa ja käynnistetään uusia kokeiluja tämän yhteistoiminnan edelleen tehostamiseksi.

6 Tehokkaat kansalliset kyberturvakyvykkyydet

Kansalliset kyberturvakyvykkyydet luovat pohjaa koko yhteiskunnan toiminnalle. Kansalliset kyberkyvykkyydet kattavat myös ne menettelyt, joilla tarvittava kyberturvallisuuden taso ja toimintaedellytykset varmistetaan. Edelleen kyberturvakyvykkyydet edistävät suvereniteettiamme kybertoimintaympäristössä sekä kansalaisten luottamusta digitaalisen yhteiskunnan toimintaan kaikissa yhteiskunnallisissa olosuhteissa. Kansallisia kyberturvakyvykkyyksiä kehitettäessä on huomioitava eri sektoreiden ja toimintojen keskinäisriippuvuudet niin kansallisella kuin kansainvälisellä tasolla sekä kansalaisten riippuvuus keskitetyistä digitaalisen yhteiskunnan palveluista. Digitaalisessa toimintaympäristössä on ensiarvoisen tärkeää, että salassa pidettävien ja henkilötietojen eheys sekä luottamuksellisuus säilyvät.

Osana kyberturvakyvykkyyksiä, arvioidaan nykyisiä viranomaisten toimintaedellytyksiä tarvittavan kansallisen kyberturvatason varmistamisessa jatkuvasti kehittyvässä kybertoimintaympäristössä, tunnistaen samalla jatkokehitystarpeet.

Osana kehittämisohjelmaa laaditaan ja käynnistetään toimenpideohjelma, jonka avulla Suomi voi hakea EU:n salaustuotteiden sertifiointeja hyväksyvän AQUA-maan (Appropriately Qualified Authority) asemaa viimeistään vuonna 2027. AQUA-statuksen saavuttaminen edistäisi merkittävästi kansallisia salauskyvykkyyksiä, edesauttaisi suomalaisten, korkealaatuisia salaustuotteita kehittävien yritysten pääsyä kansainvälisille markkinoille ja lisäisi Suomen turvallisuusviranomaisiin kohdistuvaa kansainvälistä luottamusta.

6.1 Ehdotetut kehittämistoimenpiteet

Jatkokehitetään poikkihallinnollisesti viranomaisten varautumista kyberhäiriötilanteisiin

Käynnistetään selvitystyö, jossa arvioidaan viranomaisten toimintaedellytykset kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa, ottaen huomioon kansallisen ja kansainvälisen uhkaympäristön jatkuva kehittyminen. Selvitystyön perusteella määritetään käynnistettävät toimenpiteet ja aloitetaan tarvittava säädösvalmistelu.

Kehitetään kansallisten verkkopalveluiden sisäänrakennettua turvallisuutta

Kehitetään edelleen kyberturvallisuuden kontrollipalveluita koko yhteiskunnan käyttöön osana .fi-domain -nimen käytön sisäänrakennettuja turvallisuusominaisuuksia. Tällaisia sisäänrakennettuja turvallisuusominaisuuksia on otettu jo käyttöön, mutta niitä kehitetään edelleen vastaamaan muuttuvaa uhkatilannetta.

Harmonisoidaan turvallisuusvaatimuksia ja parannetaan havainnointikykyä

Harmonisoidaan huoltovarmuuskriittisten sektoreiden ja -yritysten kyberturvavaatimuksia yhteisen turvallisuustason määrittelemiseksi, jotta eri sektoreiden keskinäisriippuvuuksista johtuvia kyberturvariskejä voidaan pienentää. Tavoitteena on näin kasvattaa yhteiskunnan sietokykyä mahdollisia kyberhyökkäyksiä vastaan. Oleellinen osa kyberturvavaatimusten ja turvallisuustason toteuttamista on valvovien viranomaisten osaamisen ja resurssien turvaaminen.

Tunnistetaan yhteiskunnan rajat ylittävät, huoltovarmuuskriittiset arvoketjut ja kehitetään niiden kyberturvallisuuden tilannekuvaa. Kehitetään operatiivisen, toimialakohtaisen ja valvovien viranomaisten tilannekuvan tuottamiseen liittyviä kyvykkyyksiä kansallisen kyberturvallisuuden tilannekuvan edelleen parantamiseksi.

Jatketaan tiivistä yhteistyötä valvovien viranomaisten, Huoltovarmuuskeskuksen Digitaalinen turvallisuus 2030 -hankkeen ja muiden yllä olevien toimenpiteiden toteuttamiseen liittyvien olennaisten kansallisten ja kansainvälisten toimijoiden kanssa.

Turvataan digitaalisen yhteiskunnan keskeiset tiedot, tietovarannot ja -palvelut

Tunnistetaan yhteiskunnan kannalta kriittiset tietovarannot, -palvelut ja -järjestelmät ja varmistetaan näiden toiminta sekä turvallisuus. Varmistetaan myös uusien, yhteiskunnan toiminnan kannalta kriittisten palveluiden turvallisuus osana niiden kehitystyötä. Näitä tehtäviä edistetään yhteistyössä Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelman 2020–2023 (Haukka) sekä Digitaalinen turvallisuus 2030 -hankkeen kanssa.

Kotimaisen salausteknologian luonti ja AQUA -statuksen saavuttaminen

Parannetaan kansallista salaustuoteperhettä sekä vakiinnutetaan kansallinen kryptostrategiatyö. Rakennetaan AQUA-statuksen saavuttamiseksi vaadittavat kyvykkyydet. Kriittisten kyberturvayhtiöiden osalta tulee varmistaa, että mahdollisissa kansallisen intressin kannalta haitallisissa määräysvallan siirtymistilanteissa sopimuksin tai olemassa olevan lainsäädännön avulla on mahdollistettu järjestelyt, joilla valtion etu voidaan turvata. Tuetaan kansallisten, kriittisten toimintaympäristöjen turvaamiseen tarkoitettujen viestintälaitteiden, ohjelmistojen ja palveluiden rakentamista sekä toteuttamista. Edistetään luodun salaustuoteperheen vientiä kansainvälisille markkinoille.

7 Seuranta ja raportointi

Jokaiselle kehittämisohjelman toimeenpanosuunnitelmassa esitetylle kehittämistoimenpiteelle on määritelty toimenpiteen edistymisen ja toteutumisen seurantaa tukevat mittarit. Kehittämistoimenpiteen toteuttamisen yhteydessä kerätään ja raportoidaan määriteltyihin mittareihin liittyvää tietoa säännöllisesti.

Mittareiden toteutumista seurataan osana toimenpiteen toteutusta sekä tämän kehittämisohjelman ohjauksen puitteissa. Kyberturvallisuusjohtaja raportoi kehittämisohjelman edistymisestä liikenne- ja viestintäministeriölle sekä Turvallisuuskomitealle kaksi kertaa vuodessa. Kehittämisohjelman edistymistä raportoidaan sidosryhmille myös laajemmin järjestelmällä seurantatilaisuuksia.

Kehittämisohjelman toimia toteutetaan pääasiassa valtion budjettiraamien sekä olemassa olevien määrärahojen puitteissa. Määrärahalisäyksiä tai muita budjettivaikutuksia vaativista toimenpiteistä päätetään erikseen valtiontalouden kehyksissä ja vuosittaisissa talousarvioissa.

Jotta varmistetaan kehittämisohjelman ajantasaisuus ja kehittämistoimenpiteiden oikea kohdennus, valtion kyberturvallisuusjohtaja koordinoi kehittämisohjelman katselmoinnin vuosittain. Tässä katselmoinnissa huomioidaan muuttunut uhka- tai riskiympäristö, muutokset kansainvälisissä verkostoissa sekä muut kehittämisohjelmaan ja sen toimenpiteisiin vaikuttavat tekijät tai trendit. Tämän arvioinnin jälkeen kehittämisohjelmaa tai sen toimeenpanosuunnitelmaa päivitetään tarvittaessa ja hyväksytetään liikenne- ja viestintäministeriössä sekä Turvallisuuskomiteassa.

Liite 1. Kehittämisohjelman toimeenpanosuunnitelma

Kehittämistoimenpiteen koordinoinnista vastaa ’vastuutahot’-sarakkeessa ensimmäisenä mainittu organisaatio.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
0	Toimeenpano	Kehittämisohjelman toimeenpano ja edistymisen seuranta ja raportointi	**LVM**	2021–2025	200 000 €/v	Kehittämisohjelman toimeenpano etenee suunnitellusti.
1	**Kansalaisten kyberturvataidot hyvälle tasolle**					
1.1	Huippuluokan osaaminen	Tietoturvapäivän toteuttaminen osana digiturvaviikkoa	**LVM**, VM	2021	Normaalit toimintamenot	Päivä on toteutettu.
1.2	Huippuluokan osaaminen	Järjestöjen roolin määrittely kansallisessa kyberturvallisuuden turvallisuusviestintätyössä ja tämän tehtävän tukeminen	**LVM**, PLM, TK-sihteeristö	2021	Normaalit toimintamenot	Järjestöillä on selkeä rooli kyberturvallisuuden turvallisuusviestintätyössä. Järjestöjä tuetaan niiden roolin mukaisesti.
1.3	Huippuluokan osaaminen	Vapaaehtoisuuteen perustuvien kyberturvayhteisöjen toimintaa tuetaan tunnistamalla mahdolliset yhteistyön muodot sekä tukemalla toimintaa mahdollisuuksien mukaan myös taloudellisesti.	**LVM**, VM, PLM, TK-sihteeristö	2021	100 000 €/v	Yhteistyömuodot on tunnistettu. Yhteistyö on käynnistetty. Toimintaa tuetaan taloudellisesti.
1.4	Huippuluokan osaaminen	Kannustetaan tyttöjä ja naisia sekä muita aliedustettuja ryhmiä kiinnostumaan kyberalasta.	**LVM**, TEM, SM, TK-sihteeristö, Kyberala (FISC)	2021–2024	Normaalit toimintamenot	Nykytila ja tarvittavat kehittämistoimenpiteet on tunnistettu. Kehittämistoimenpiteitä on toteutettu. Opintoihin on hakeutunut ja alalle on työllistetty nykyistä enemmän naisia.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
1.5	Huippuluokan osaaminen	Järjestöjä tuetaan vakavien kyberhyökkäystilanteiden jälkihoitoon liittyvissä valmiuksissa sekä näiden toteutuksessa yhteistyössä viranomaisten kanssa.	**LVM**, PLM, TK-sihteeristö	2021	Normaalit toimintamenot	Toimintamalli on määritelty Valmiudet luotu.
1.6	Huippuluokan osaaminen	Kansalaisille kohdistetun kyberturvallisuustietoisuuden viestintäsuunnitelman laatiminen.	**LVM**, VM, TK-sihteeristö	2021	Normaalit toimintamenot	Kansalaisten kyberturvallisuus tietoisuuden kasvattamiseen tähtäävä viestintäsuunnitelma on luotu ja sen mukainen toiminta on käynnistynyt.
2	**Kyberturvallisuuden koulutuksen kehittäminen**					
2.1	Huippuluokan osaaminen	Koulutusohjelmien muutostarpeiden tunnistaminen yhteistyössä korkeakoulujen kanssa.	**LVM**, TEM, OKM	Selvitetään aikataulu	450 000 €/ tutkimus	Kyberturvallisuuden koulutukseen liittyvät muutostarpeet on tunnistettu.
2.2	Huippuluokan osaaminen	Mahdollisuuksien mukaan varhaiskasvatuksessa luodaan perusteet lapsille ymmärtää, kuinka käyttää turvallisesti digitaalisen yhteiskunnan tuotteita ja palveluita.	**OKM**	Selvitetään aikataulu	Normaalit toimintamenot	Mahdolisuuksien mukaan kyberturvaopinnot sisällytetään varhaiskasvatuksen suunnitelmiin.
2.3	Huippuluokan osaaminen	Harkitaan kyberturvallisuuden sisällyttämistä peruskoulun opetussuunnitelmaan.	**OKM**	Selvitetään aikataulu	Normaalit toimintamenot	Harkitaan kyberturvaopintojen sisällytämistä opetussuunnitelmaan, tutkimuksen pohjalta.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
2.4	Huippuluokan osaaminen	Mahdollisuuksien mukaan lukiokoulutuksessa laajennetaan ja syvennetään em. taitoja ja luodaan perustaa alan erityisosaamiselle korkea-asteen koulutuksessa.	**OKM**	Selvitetään aikataulu	Normaalit toimintamenot	Mahdollisuuksien mukaan kyberturvallisuus opinnot sisällytetetään opetussuunnitelmaan, tutkimuksen pohjalta.
2.5	Huippuluokan osaaminen	Ammatilliseen koulutukseen pyritään sisällyttämään kyberturvallisuuden alan perusammattitaitoon tähtäävät opinnot.	**OKM**	Selvitetään aikataulu	Normaalit toimintamenot	Mahdollisuuksien mukaan kyberturvallisuus opinnot sisällytetään opetussuunnitelmaan, tutkimuksen pohjalta.
2.6	Huippuluokan osaaminen	Ammatillisen ja täydentävän kyberturvaosaamisen kehittämiseksi pyritään suunnitelelemaan osaamispolkuja, joissa hyödynnetään olemassa olevia ja luodaan tarvittaessa uusia sisältöjä.	**OKM**	Selvitetään aikataulu	Normaalit toimintamenot	Pyritään luomaan kyberturvallisuuden opintopolkuja, tutkimuksen pohjalta.
2.7	Huippuluokan osaaminen	Huippu- ja erityisosaamistarpeet tunnistetaan ja osaamista kehitetään tarpeiden mukaisesti.	**OKM**, LVM, TEM, Kyberala (FISC), PLM, SM	Selvitetään aikataulu	Normaalit toimintamenot	Tarpeet on tunnistettu ja osaamisen kehittäminen on mahdollistettu.
2.8	Huippuluokan osaaminen	Viranomaisten yhteisiä kyberturvakoulutuksia järjestetään keskitetysti.	**LVM**, PLM, SM	Selvitetään aikataulu	600 000 €/v	Yhteisiä koulutuksia on järjestetty.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
2.9	Huippuluokan osaaminen	Toteutetaan jo tunnistetut keinot, ml. lupaprosessin sujuvoittaminen, nopeuttamaan ja helpottamaan kansainvälisten kyberturvallisuusammattilaisten rekrytointia suomalaisen elinkeinoelämän palvelukseen sekä huippuosaajia alan tutkimus- ja opetustyöhön	**SM**, TEM, Kyberala (FISC)	2021–2025	Normaalit toimintamenot	Lupaprosesseja on sujuvoitettu. Kansainvälisiä huippuosaajia on rekrytoitu.
3	**Kyberturvallisuuden harjoitustoiminnan yhteistyön vahvistaminen**					
3.1	Kiinteä yhteistyö	Yhteistyö viranomaisten, elinkeinoelämän ja järjestöjen välillä kriittisten arvoketjun turvaamiseen liittyvässä harjoitustoiminnassa.	**LVM**, PLM, VM HVK, TK-sihteeristö	2021–2023	Normaalit toimintamenot	Vähintään yksi harjoitus järjestetty per arvoketju joka toinen vuosi.
3.2	Kiinteä yhteistyö	Yhteisten kyberharjoitusympäristöjen hyödyntäminen ja niiden toiminnan varmistaminen sekä pokkihallinnollinen ohjaus	**LVM**, VM, PLM, SM	2021–2025	1 milj. €/v	Tarvittavat harjoitusympäristöt ovat käytössä ja neljä harjoitusta vuodessa on järjestetty.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
4	**Kansallisen kyberturvallisuuden tutkimus- ja kehittämisyhteistyön edistäminen**					
4.1	Kiinteä yhteistyö	Kyberturvallisuuden tutkimus- ja kehittämisyhteistyötä koordinoidaan ja kotimaiseen kyberturvatutkimukseen kohdistetaan rahoitusta yhteisten tavoitteiden saavuttamiseksi	**TEM**, OKM, LVM, PLM, SM,	2021–2025	1 mil. €/v	Koordinaatiomalli on luotu. Yhteiset tavoitteet on tunnistettu. Kotimaisen kyberturvatutkimuksen rahoitus on turvattu.
4.2	Kiinteä yhteistyö	Käynnistetään Valtionhallinnon kyberturvayhteisöjä aktivoivia toimia, kuten turvallisen ohjelmistokoodin kehittäminen ja soveltuvin osin Bug Boynty -ohjelmia digitaalisten palveluiden kyberturvallisuuden jatkuvaksi parantamiseksi	**VM**, LVM, VNK, Kaikki ministeriöt	Jatkuva	100 000 €/ suunnittelutyö	Kyberturvayhteisöjä aktivoivia toimia on käynnistetty ja Bug Bounty-ohjelmat ovat käynnissä.
4.3	Kiinteä yhteistyö	Tunnistetaan mahdollisuudet tutkimustulosten kaupallistamiseen ja tuetaan tätä.	**TEM**, VM, PLM, Kyberala (FISC)	Jatkuva	Normaalit toimintamenot	Kaupallistamiseen johtavia tutkimustuloksia on syntynyt.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
5	**Aktiivinen osallistuminen ja vaikuttaminen kansalliseen ja kansainväliseen kyberturvallisuuden yhteistyöhön**					
5.1	Kiinteä yhteistyö	Osallistutaan aktiivisesti kansainväliseen kyberturvayhteistyöhön. Kyberturvateollisuudelle luodaan mahdollisuudet osallistua yhteisen kannan valmisteluun teema-alueittain perustettavien työryhmien avulla.	**UM**, TEM, LVM, PLM, VM Kyberala (FISC)	Jatkuva	Normaalit toimintamenot	Vaikuttaminen on aktiivista kaikissa merkittävissä kansainvälisissä yhteistyö-foorumeissa. Osallistumisen vaikuttavuutta arvioidaan vuosittain jokaisen yhteistyöfoorumin osalta.
5.2	Kiinteä yhteistyö	Suomen menestymistä kansainvälisellä kyberturvakentällä seurataan kansainvälisiin indekseihin perustuen	**VM**, LVM, TK-sihteeristö, kaikki ministeriöt	Jatkuva	Normaalit toimintamenot	Seurantaa, tehdään, tuloksiin reagoidaan ja Suomi kykenee tason nostoon vuosittain (GCI- ja NCSI -indeksi).
6	**Kotimaisten kyberturvatuotteiden ja -palveluiden kasvun ja kansainvälistymisen tukeminen**					
6.1	Vahva kotimainen kyberteollisuus	Laaditaan kyberturvallisuusalan kasvustrategia, joka tukee myös Suomeen tehtäviä kansainvälisiä investointeja.	**TEM**, kyberala (FISC)	2021	Normaalit toimintamenot	Kasvustrategia on luotu ja sen toimeenpano on käynnistetty.
6.2	Vahva kotimainen kyberturvateollisuus	Kotimaisen kyberturvateollisuuden innovaatioita, tuotteita ja ratkaisuita hyödynnetään laajemmin.	**TEM**, VM, PLM, kaikki ministeriöt, Kyberala (FISC)	Jatkuva	Normaalit toimintamenot	Kotimaisten kyberturvatuotteiden ja palveluiden kansallinen markkinaosuus kasvaa vuosittain.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
6.3	Vahva kotimainen kyberturvateollisuus	Kehitetään hankintaosaamista kyberturvallisuuden tuotteiden ja palveluiden ostoon.	**VM**, TEM, PLM, Kyberala (FISC)	2021–2022	Normaalit toimintamenot	Kyberturvallisuuden tuotteiden ja palveluiden hankintaosaamisen kasvattamiseen on kohdistettu koulutuksia ja annettu soveltamisohjeita.
6.4	Vahva kotimainen kyberturvateollisuus	Aktivoidaan Suomen edustustoja kansainväliseen yhteistyöhön suomalaisen osaamisen tunnettuuden edistämiseksi.	**UM**, TEM, Kyberala (FISC)	Jatkuva	Normaalit toimintamenot	Yhteistyötä edustustojen kanssa on lisätty ja suomalaista kyberturvallisuusosaamista on markkinoitu laajasti.
6.5	Vahva kotimainen kyberturvateollisuus	Kehitetään kansallista tiedonvaihtoa, jotta Suomen kyberturvaetuja ja edunvalvontaa voidaan ajaa hajautetusti, mutta yhtenä rintamana ja yhtenäisellä viestillä eteenpäin.	**UM**, TEM, PLM, Kyberala (FISC)	Jatkuva	Normaalit toimintamenot	Eri kansainvälisiin yhteistyöfoorumeihin osallistuvat organisaatiot ovat tehostaneet keskinäistä tiedonvaihtoaan.
6.6	Vahva kotimainen kyberturvateollisuus	Tuetaan tuotteiden ja palveluiden tuotteistamista ja konseptointia kansainvälisen markkinan näkökulmasta.	**TEM**, Kyberala (FISC)	Jatkuva	Normaalit toimintamenot	Tuettaistamiseen ja markkinointiin on kehitetty toimintamalleja sekä kansainvälistymiseen tähtäävän kasvun konsepti on saatavilla.
6.7	Vahva kotimainen kyberturvateollisuus	Hyödynnetään Suomen vahvuuksia kansainvälistymisessä ja markkinoinnissa.	**Kaikki ministeriöt,** Kyberala (FISC)	Jatkuva	Normaalit toimintamenot	Yhteinen agenda ja tavoitteet on luotu ja Suomen vahvuuksia on edistetään aktiivisesti kansainvälisillä areenoilla.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
6.8	Vahva kotimainen kyberturvateollisuus	Perustetaan kyberturvallisuuden kasvu- ja osaamiskeskus	**TEM**, Kyberala (FISC), Kansallinen koordinaatio-keskus	2021–2023	Normaalit toimintamenot	Kasvu- ja osaamiskeskuksen työ on edistänyt kyberteollisuuden yritysten kasvua, osaamista ja kansainvälistä kilpailukykyä.
7	**Uusien kyberturvayritysten perustamisen edistäminen**					
7.1	Vahva kotimainen kyberturvateollisuus	Tuetaan eri elinkaaren vaiheissa olevien kyberturvayritysten syntyä, kehittymistä ja kasvua.	**TEM**, Kyberala (FISC), Kansallinen koordinaatio-keskus	2021–2025	Normaalit toimintamenot	Uusien yritysten ja kansallisen sekä kansainvälisen kasvun mahdollistama konsepti (elinkaarimalli) on luotu, viestitty ja sitä toteutetaan aktiivisesti.
7.2	Vahva kotimainen kyberturvateollisuus	Yritykset tarvitsevat myös kotimaista rahoitusta sekä pääomia mukaan lukien mahdolliset valtion rahoitus- ja omistusosuudet.	**TEM**, VNK, LVM, Kyberala (FISC), Kansallinen koordinaatio-keskus	Jatkuva	Normaalit toimintamenot	Kansallisia pääomia on saatavilla riittävästi kasvun mahdollistamiseksi.
7.3	Vahva kotimainen kyberturvateollisuus	Jatketaan ja edelleen tiivistetään yhteistyötä mm. Business Finlandin, Kyberturva-alan sekä muiden tarvittavien yhteistyötahojen kanssa.	**TEM**, VM, Kyberala (FISC)	Jatkuva	Normaalit toimintamenot	Yhteistyö on johtanut kansainvälistymisasteen kasvuun.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
7.4	Vahva kotimainen kyberturvateollisuus	Kehitetään kyberturvallisuuteen liittyvien julkisten hankintojen innovatiivisuutta ja kokeiluja yhteistyössä työ- ja elinkeinoministeriön Keino-hankkeen kanssa huomioiden TKI-hankinnat.	**TEM**, LVM, VM,PLM, Kyberala (FISC)	2021–2022	Normaalit toimintamenot	Kokeilut ja innovatiiviset hankinnat ovat kasvaneet sekä yhteistyö Keino-hankkeen kanssa on käynnnissä.
7.5	Vahva kotimainen kyberturvateollisuus	Käynnistetään pilottihanke kyberturvallisuuden osa-alueella yhteistyössä työ- ja elinkeinoministeriön KEINO-hankkeen ja vaikuttavuusinvestoimisen osaamiskeskuksien kanssa.	**TEM**, LVM, VM, Kyberala (FISC),	2021–2024	Normaalit toimintamenot	Pilottihanke on toteutettu.
8	**Jatkokehitetään poikkihallinnollisesti viranomaisten varautumista laajoihin kyberhäiriötilanteisiin**					
8.1	Tehokkaat kansalliset kyberturvakyvykkyydet	Käynnistetään selvitystyö, jossa arvioidaan viranomaisten toimintaedellytykset kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa ja kyberpuolustuksessa.	**SM** ja PLM, muut tarvittavat tahot	2021–2023	Täydennetään selvitystyön valmistuttua.	Selvitystyön perusteella määritetään käynnistettävät toimenpiteet ja aloitetaan tarvittava säädösvalmistelu.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
9	**Kehitetään kansallisten verkkopalveluiden sisäänrakennettua turvallisuutta**					
9.1	Tehokkaat kansalliset kyberturvakyvykkyydet	Kehitetään edelleen kyberturvallisuuden kontrollipalveluita koko yhteiskunnan käyttöön osana .fi-domain -nimen käytön sisäänrakennettuja turvallisuusominaisuuksia.	**LVM**	2021–2022	Normaalit toimintamenot	Uusia turvallisuus-ominaisuuksia on käyttöönotettu mahdollisuuksien mukaan.
10	**Harmonisoidaan turvallisuusvaatimuksia ja parannetaan havainnointikykyä**					
10.1	Tehokkaat kansalliset kyberturvakyvykkyydet	Määritellään huoltovarmuuskriittisten sektoreiden ml. yritykset kyberturvallisuusvaatimuksille yhteinen vähimmäistaso.	**HVK**, kaikki ministeriöt	2021–2022	Normaalit toimintamenot	Yhteinen vähimmäistaso on tunnistettu saatettu voimaan eri sektoreissa.
10.2	Tehokkaat kansalliset kyberturvakyvykkyydet	Tunnistetaan yhteiskunnan rajat ylittävät, huoltovarmuuskriittiset arvoketjut ja kehitetään kyberturvallisuuden tilannekuvia näiden arvoketjujen osalta.	**HVK**	Jatkuva	Normaalit toimintamenot	Arvoketjut on tunnistettu ja tilannekuvakyvykkyyksiä kehitetty vastaten tarpeita.
10.3	Tehokkaat kansalliset kyberturvakyvykkyydet	Kehitetään operatiivisen, toimialakohtaisen ja valvovien viranomaisten tilannekuvan tuottamiseen liittyviä kyvykkyyksiä kansallisen kyberturvallisuuden tilannekuvan parantamiseksi.	**HVK**, LVM, sektori-kohtaiset NIS -viranomaiset	Jatkuva	Normaalit toimintamenot	Toimialakohaisten valvovien viranomaisten tilannekuvakyvykkyyksille on asetettu yhteinen tavoite, kyvykkyydet tunnistettu, toimintaa on kehitetty ja jatkuva toiminta on käynnissä.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
11	**Turvataan digitaalisen yhteiskunnan keskeiset tiedot, tietovarannot ja -palvelut**					
11.1	Tehokkaat kansalliset kyberturvakyvykkyydet	Tunnistetaan yhteiskunnan kannalta kriittiset tietovarannot, -palvelut ja -järjestelmät ja varmistetaan näiden toiminta sekä turvallisuus.	**VM**, HVK	Jatkuva	200 000 €/ selvitystyö	Tietovarannot, palvelut ja -järjestelmät on tunnistettu ja niiden saatavuus ja turvallisuus on varmistettu koko elinkaaren ajan (kehitys, tuotanto, tuotannosta poisto).
11.2	Tehokkaat kansalliset kyberturvakyvykkyydet	Varmistetaan uusien, yhteiskunnan toiminnan kannalta kriittisten palveluiden turvallisuus osana niiden kehitystyötä.	**HVK**, VM	Jatkuva	Normaalit toimintamenot	Yhteiskunnan toiminnan kannalta kriittisten palveluiden turvallinen ohjelmistokehitysprosessi on luotu, sitä kehitetään ja noudatetaan. Palveluien asianmkainen. sisäänrakennettu turvallisuus varmistetaan ennen käytöönottoa.

Tunniste	Teema	Kehittämistoimenpide	Vastuutahot	Aikataulu	Rahoitus	Mittarit
12	**Kotimaisen salausteknologian luonti ja AQUA -statuksen saavuttaminen**					
12.1	Tehokkaat kansalliset kyberturvakyvykkyydet	Parannetaan kansallista salaustuoteperhettä sekä vakiinnutetaan krypto-strategiatyö	**LVM**, Kyberala (FISC), PLM	2021–2026	2 milj. €/v	Kansallinen salaustuoteperhe on valmis.
12.2	Tehokkaat kansalliset kyberturvakyvykkyydet	Rakennetaan AQUA-statuksen saavuttamiseksi vaadittavat kyvykkyydet.	**LVM**, Traficom, VTT	2021–2026	1 milj. €/v	Vaadittavat kyvykkyydet on rakennettu.
12.3	Tehokkaat kansalliset kyberturvakyvykkyydet	Tunnistetaan kansallisen turvallisuuden näkökulmasta kriittiset kyberturvallisuusyhtiöt ja varmistetaan, että mahdollisissa kansallisen intressin kannalta haitallisissa määräysvallan siirtymistilanteissa sopimuksin tai olemassa olevan lainsäädännön avulla on mahdollistettu järjestelyt, joilla valtion etu voidaan turvata	**TEM**, VNK, VM, LVM, HVK	Jatkuva	Normaalit toimintamenot	Kansallisesti kriittiset kyberturvayhtiöt on tunnistettu ja omistusosuudet varmistettu.

Liite 2. Kehittämistoimenpiteiden vaikuttavuusanalyysi

ID	Teema	Kehittämis-toimenpide	Nykytila	Tavoitetila	Vaikutukset	Arvio kokonais-vaikutuksista	Ehdotetut tehtävät toimenpiteen toteuttamiseksi
0	Toimeenpano	Kehittämis-ohjelman toimeenpano	Kehittämisohjelma kuvaa toimenpiteet kansallisen kyberturvallisuuden kokonaistilan parantamiseksi.	Kehittämisohjelmaa toteutetaan suunnitellusti aikataulun mukaan. Kehittämisohjelmaa arvioidaan säännöllisesti ja sitä päivitetään vastaamaan muuttuvaa kokonaistilannetta. Vuosittainen investointitarve 200 000 €	Kansallinen	Erittäin suuri	* Kehittämisohjelman toteuttaminen suunnitellusti. * Kehittämisohjelman säännöllinen arviointi ja päivitys.
1	Huippuluokan osaaminen	Kansalaisten kyberturvataidot hyvälle tasolle	Kyberturvallisuuden kansalaistaidot eivät ole riittävällä tasolla digitalisaation nykyisiin vaatimuksiin nähden.	Tavoitetilassa jokaisella kansalaisella lapsesta eläkeläiseen on riittävät taidot toimia digitaalisessa yhteiskunnassa. Yhteisöjen tukemiseen kohdennetulla investoinnilla 100 000 €/v voidaan varmistaa mm. tarvittavien käytännön kulujen kattamista. Tällä nähdään olevan toiminnan jatkuvuuden varmistamisen näkökulmasta merkittävä vaikutus.	Kansainvälinen	Suuri	* Kyberturvapäivän toteuttaminen osana digiturvaviikkoa. * Järjestöjen roolin määrittely kansallisessa kyberturvallisuuden turvallisuusviestintätyössä ja tämän tehtävän tukeminen. * Vapaaehtoisuuteen perustuvien kyberturvayhteisöjen toimintaa tuetaan tunnistamalla mahdolliset yhteistyön muodot. Toimintaa myös tuetaan taloudellisesti mahdollisuuksien mukaan. * Järjestöjä tuetaan vakavien kyberhyökkäystilanteiden jälkihoitoon liittyvissä valmiuksissa sekä näiden toteutuksessa yhteistyössä viranomaisten kanssa.
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	Suuri	
					Organisaatio / Yritys	Erittäin suuri	
					Kansalainen	Erittäin suuri	

ID	Teema	Kehittämis-toimenpide	Nykytila	Tavoitetila	Vaikutukset	Arvio kokonais-vaikutuksista	Ehdotetut tehtävät toimenpiteen toteuttamiseksi
2	Huippuluokan osaaminen	Kyber-turvalli-suuden koulutuksen kehittäminen	Koulutusohjelmiin ei ole sisällytetty riittä-västi elinkeinoelämän ja yhteiskunnan tar-peita tukevia kyberturvallisuuden opintoja. Koulutusohjelmat eivät nykytilassa valmista asiantuntijoita em. tarpeisiin ja asiantuntijat koulutetaan vasta työelämään astumisen jälkeen.	Koulutusohjelmien sisällöt ja oppimispolut olisi suunniteltu siten, että koulutusohjelmat tuottaisivat jo valmiimpia asiantuntijoita elinkeinoelämän ja yhteiskunnan tarpeisiin. Lisäksi tarjolla olisi riittävä määrä osaamisen päivittämiseen ja erityisalojen kyberturvallisuuteen liittyviä opintoja. Tämän tavoitteen toteuttaminen vaatii laajan selvitystyön, jonka kustannuksiksi arvioidaan 450 000 €. Selvitystyön vaikutukset nähdään erittäin tärkeänä koko koulutusjärjestelmän sekä kyberturvallisuusosaamisen kehittämisen osalta. Edelleen viranomaisten kyberturvallisuuden koulutuksien nykyistä tiiviimpi keskittäminen luo parempia mahdollisuuksia osaamisen jatkuvaan kehittämiseen sekä toteuttamiseen kansallisesti. Tämän toteuttamiseen arvioidut investoinnit ovat vuositasolla 600 000 €.	Kansainvälinen	Suuri	* Varhaiskasvatuksessa pyritään luomaan perusteet lapsille ymmärtää, kuinka käyttää turvallisesti digitaalisen yhteiskunnan tuotteita ja palveluita. Tutkimuksen pohjalta, mahdollisuuksien mukaan, kyberturvallisuus sisällytetään peruskoulun opetussuunnitelmaan ja lukiokoulutuksessa pyritään laajentamaan ja syventämään em. taitoja ja pyritään luomaan perustaa alan erityisosaamiselle korkea-asteen koulutuksessa. Pyritään sisällyttämään ammatilliseen koulutukseen kyberturvallisuuden alan perusammattitaitoon tähtäävät opinnot. * Ammatillisen ja täydentävän kyberturvaosaamisen kehittämiseksi pyritään suunnittelemaan osaamispolkuja, joissa hyödynnetään olemassa olevia ja luodaan tarvittaessa uusia sisältöjä. * Huippu- ja erityisosaamistarpeet tunnistetaan ja osaamista kehitetään tarpeiden mukaisesti. * Yhteisiä kyberturvakoulutuksia järjestetään keskitetysti
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	Erittäin suuri	
					Organisaatio / Yritys	Erittäin suuri	
					Kansalainen	Merkittävä	

ID	Teema	Kehittämis-toimenpide	Nykytila	Tavoitetila	Vaikutukset	Arvio kokonais-vaikutuksista	Ehdotetut tehtävät toimenpiteen toteuttamiseksi
3	Kiinteä yhteistyö	Kyber-turvallisuuden harjoitus-toiminnan yhteistyön vahvistaminen	Kyberturvallisuuden harjoitustoiminta on tällä hetkellä hajanaista ja toimijat harjoittelevat kukin omiin, erillisiin skenaarioihin liittyen. Elinkeinoelämän ja järjestöjen panosta harjoitustoiminnassa ei hyödynnetä tällä hetkellä riittävästi.	Kyberturvallisuuden harjoitustoiminnassa tehdään entistä tiiviimpää yhteistyötä siten, että elinkeinoelämä on tiiviisti mukana huoltovarmuuskriittisestä näkökulmasta ja järjestöjen rooli on merkittävämpi. Yhteisiä pitkäaikaisia uhkaskenaarioita sekä kyberharjoitusympäristöjä hyödynnetään tavoitteellisesti. Yhteisiin harjoitusympäristöihin investointi luo varmuutta ympäristöjen toiminnan jatkuvuuden sekä ajantasaisuuden varmistamiselle. Nämä nähdään erittäin merkittävänä osaamisen ja yhteistyön ylläpidossa sekä kehittämisessä. Vuosittaisiksi investoinneiksi arvioidaan 1 milj. €.	Kansainvälinen	-	* Yhteistyö viranomaisten, elinkeinoelämän ja järjestöjen välillä kriittisten arvoketjun turvaamiseen liittyvässä harjoitustoiminnassa. * Yhteisten kyberharjoitusympäristöjen hyödyntäminen ja niiden toiminnan varmistaminen.
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	Suuri	
					Organisaatio / Yritys	Suuri	
					Kansalainen	-	

ID	Teema	Kehittämis-toimenpide	Nykytila	Tavoitetila	Vaikutukset	Arvio kokonais-vaikutuksista	Ehdotetut tehtävät toimenpiteen toteuttamiseksi
4	Kiinteä yhteistyö	Kansallisen kyberturvallisuuden tutkimus- ja kehittämisyhteistyön edistäminen	Kyberturvallisuuden tutkimusta tehdään, mutta sitä ei koordinoida yhteisten tavoitteiden saavuttamiseksi. Tutkimustulosten kaupallistamisessa on haasteita. Tutkimusrahoitusta ei ole saatavilla riittävästi.	Kyberturvallisuuden tutkimus- ja kehittämisyhteistyötä koordinoidaan yhteisten tavoitteiden saavuttamiseksi. Kybertutkimuksen kotimaisen rahoituksen riittävyyttä tuetaan. Teoreettisten tutkimustulosten lisäksi tunnistetaan entistä enemmän mahdollisuuksia tulosten suoraan kaupallistamiseen ja tuetaan näiden edistämistä. Yhteisö tukee kyberturvallisuuden jatkuvaa parantamista. Kansallisen kyberturvallisuustutkimus- ja kehittämistyön rooli nähdään erittäin merkittävänä. Tutkimus luo potentiaalia uusille innovaatioille sekä kasvulle. Tälle työlle on arvioitu vuosittaiseksi investointitarpeeksi 1 milj. €. Eri yhteisöjen aktivoinnissa nähdään merkittäviä mahdollisuuksia myös digitalisen yhteiskunnan kyberturvallisuuden kehittämisessä. Yhteisön aktivointi vaatii yhteiset pelisäännöt ja toimintamallit. Niiden toteuttamisen investointitarpeiksi arvioidaan 100 000 €.	Kansainvälinen	-	* Kyberturvallisuuden tutkimus- ja kehittämisyhteistyötä koordinoidaan yhteisten tavoitteiden saavuttamiseksi * Käynnistetään Valtionhallinnon turvallisen ohjelmistokoodin kehittämiseen ja digitaalisten palveluiden turvallisuuden parantamiseen yhteisöllisiä toimia. * Kybertutkimuksen kotimaisen rahoituksen riittävyyttä tuetaan. * Tunnistetaan mahdollisuudet tutkimustulosten kaupallistamiseen ja tuetaan tätä.
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	Erittäin suuri	
					Organisaatio / Yritys	Suuri	
					Kansalainen	-	

ID	Teema	Kehittämis-toimenpide	Nykytila	Tavoitetila	Vaikutukset	Arvio kokonais-vaikutuksista	Ehdotetut tehtävät toimenpiteen toteuttamiseksi
5	Kiinteä yhteistyö	Aktiivinen osallistuminen ja vaikuttaminen kansalliseen ja kansainväliseen kyberturvallisuuden yhteistyöhön	Kaikkia kansallisen ja kansainvälisen yhteistyön mahdollisuuksia ei nykytilassa hyödynnetä tehokkaasti.	Suomi osallistuu kyberturvallisuusstrategiassa mainittujen järjestöjen yhteistyöhön, kehittää kansallista tiedonvaihtoa sekä edistää kansainvälistä yhteistyötä mm. lähetystöjen kautta.	Kansainvälinen	Erittäin suuri	* Osallistutaan aktiivisesti kansainväliseen kyberturvayhteistyöhön * Suomen menestymistä kansainvälisellä kyberturvakentällä seurataan kansainvälisiin indekseihin perustuen
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	-	
					Organisaatio / Yritys	Merkittävä	
					Kansalainen	-	
6	Vahva kotimainen kyberturvateollisuus	Kotimaisten kyberturvatuotteiden ja -palveluiden kasvun ja kansainvälistymisen tukeminen	Kotimaisille kyberturvatuotteille tarjottavaa tukea erityisesti kansainvälistymisen ja kasvun saavuttamiseksi tulee kehittää edelleen.	Kansallisesta markkinasta kansainväliseen markkinaan siirtymiselle on saatavissa tukea ja rahoitusta. Suomen vahvuuksia hyödynnetään aktiivisesti markkinoinnissa ja omalla ostokäyttäytymisellä tuetaan tuotteiden kehittämistä. Kansalliselle kyberturvateollisuudelle luodaan kasvustrategia, joka huomioi myös Suomeen kohdistettavat kansainväliset, kyberekosysteemiä vahvistavat, investoinnit.	Kansainvälinen	Erittäin suuri	*Luodaan kansalliselle kyberturvateollisuudelle kasvustrategia *Kotimaisen kyberturvateollisuuden innovaatioita, tuotteita ja ratkaisuita hyödynnetään laajemmin. * Kehitetään hankintaosaamista kyberturvallisuuden tuotteiden ja palveluiden ostoon. * Aktivoidaan Suomen edustustoja kansainväliseen yhteistyöhön suomalaisen osaamisen tunnettuuden edistämiseksi. * Kehitetään kansallista tiedonvaihtoa, jotta Suomen kyberturvaetuja ja edunvalvontaa voidaan ajaa hajautetusti, mutta yhtenä rintamana ja yhtenäisellä viestillä eteenpäin. * Tuetaan tuotteiden ja palveluiden tuotteistamista ja konseptointia kansainvälisen markkinan näkökulmasta. * Hyödynnetään Suomen vahvuuksia kansainvälistymisessä ja markkinoinnissa.
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	Suuri	
					Organisaatio / Yritys	Erittäin suuri	
					Kansalainen	Merkittävä	

ID	Teema	Kehittämis-toimenpide	Nykytila	Tavoitetila	Vaikutukset	Arvio kokonais-vaikutuksista	Ehdotetut tehtävät toimenpiteen toteuttamiseksi
7	Vahva kotimainen kyberturva-teollisuus	Uusien kyber-turvayritysten perustamisen edistäminen	Uusien kyberturvayritysten perustamiseen liittyvää tukea tulee edelleen kehittää tuotteistamisen ja rahoituksen osalta, huomioiden yritysten eri elinkaaren vaiheet.	Kyberturvateollisuudelle on tarjolla riittävästi pääomia ja rahoitusta. Elinkaaren eri vaiheissa olevien yritysten toimintaa tuetaan sopivin tavoin.	Kansainvälinen	-	* Tuetaan eri elinkaaren vaiheissa olevien kyberturvayritysten syntyä, kehittymistä ja kasvua tulee. * Yritykset tarvitsevat myös kotimaista rahoitusta sekä pääomia mukaan lukien mahdolliset valtion rahoitus- ja omistusosuudet. * Jatketaan ja edelleen tiivistetään yhteistyötä mm. Business Finlandin, Kyberalan (FISC) sekä muiden tarvittavien yhteistyötahojen kanssa. * Kehitetään kyberturvallisuuteen liittyvien julkisten hankintojen innovatiivisuutta ja kokeiluja yhteistyössä työ- ja elinkeinoministeriön Keino-hankkeen kanssa huomioiden TKI-hankinnat. * Käynnistetään pilottihanke kyberturvallisuuden osa-alueella yhteistyössä työ- ja elinkeinoministeriön KEINO-hankkeen ja vaikuttavuusinvestoimisen osaamiskeskuksien kanssa
					Kansallinen	Suuri	
					Hallinnonala / Toimiala	Suuri	
					Organisaatio / Yritys	Erittäin suuri	
					Kansalainen	Merkittävä	

ID	Teema	Kehittämis-toimenpide	Nykytila	Tavoitetila	Vaikutukset	Arvio kokonais-vaikutuksista	Ehdotetut tehtävät toimenpiteen toteuttamiseksi
8	Tehokkaat kansalliset kyberturva-kyvykkyydet	Jatkokehitetään poikkihallinnollisesti viranomaisten varautumista laajoihin kyberhäiriötilanteisiin	On tunnistettu tarve kartoittaa ja jatkokehittää viranomaisten varautumista laajoihin kyberhäiriötilanteisiin.	Viranomaisten toimintaedellytykset kansallisen kyberturvallisuuden varmistamisessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta on selvitetty. Selvityksessä arvioidaan viranomaisten toimintaedellytykset kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa ja kyberpuolustuksessa. Nykytilan arvioinnin merkitys on erittäin suuri. Arviointityö on laaja kattaen käytännössä kaikkien toimintaedellytysten arvioinnin. Arvioinnissa esiin tulleiden kehitystarpeiden toiminnallistaminen on puolestaan keskeistä tämän toimenpiteen vaikuttavuuden varmistamiseksi. Toimenpiteet ja investointitarpeet tarkentuvat selvitystyön valmistuttua.	Kansainvälinen	-	Selvitystyön perusteella määritetään käynnistettävät toimenpiteet ja aloitetaan tarvittava säädösvalmistelu.
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	Erittäin suuri	
					Organisaatio / Yritys	Suuri	
					Kansalainen	-	

ID	Teema	Kehittämis-toimenpide	Nykytila	Tavoitetila	Vaikutukset	Arvio kokonais-vaikutuksista	Ehdotetut tehtävät toimenpiteen toteuttamiseksi
9	Tehokkaat kansalliset kyberturva-kyvykkyydet	Kehitetään kansallisten verkko-palveluiden si-säänrakennettua turvallisuutta	On tunnistettu tarve kehittää kansallisten verkkopalveluiden sisäänrakennettua turvallisuutta.	Verkkopalvelut on suunniteltu siten, että niihin on sisäänrakennettu turvallisuuspalveluita.	Kansainvälinen	-	* Kehitetään edelleen kyberturvallisuuden kontrollipalveluita koko yhteiskunnan käyttöön osana .fi-domain -nimen käytön sisäänrakennettuja turvallisuusominaisuuksia.
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	Erittäin suuri	
					Organisaatio / Yritys	Erittäin suuri	
					Kansalainen	-	
10	Tehokkaat kansalliset kyberturvaky-vykkyydet	Harmonisoidaan turvallisuus-vaatimuksia ja parannetaan ha-vainnointikykyä	Huoltovarmuuskriittisten sektoreiden turvallisuus-vaatimukset eroavat toisistaan. Tarve havain-nointikyvyn ja tilanne-kuvan muodostamiseen liittyvien kyvykkyyksien kehittämiseen on tunnis-tettu.	Huoltovarmuuskriittisten sektoreiden turvallisuusvaatimukset on kartoitettu ja varmistettu, että niillä saavutetaan riittävä turvallisuuden taso. Operatiivisen tilannekuvan muodostamiseen liittyvät kyvykkyydet ovat olemassa, siten että kansallinen, kyberturvallisuuden tilannekuva voidaan muodostaa.	Kansainvälinen	-	* Määritellään huoltovarmuuskriittisten sektoreiden ml. yritykset kyberturvavaatimuksille yhteinen vähimmäistaso, * Tunnistetaan yhteiskunnan rajat ylittävät, huoltovarmuuskriittiset arvoketjut ja kehitetään kyberturvallisuuden tilannekuvia näiden arvoketjujen osalta. * Kehitetään operatiivisen, toimialakohtaisen ja valvovien viranomaisten tilannekuvan tuottamiseen liittyviä kyvykkyyksiä kansallisen kyberturvallisuuden tilannekuvan parantamiseksi
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	Erittäin suuri	
					Organisaatio / Yritys	-	
					Kansalainen	-	

ID	Teema	Kehittämis-toimenpide	Nykytila	Tavoitetila	Vaikutukset	Arvio kokonais-vaikutuksista	Ehdotetut tehtävät toimenpiteen toteuttamiseksi
11	Tehokkaat kansalliset kyberturvaky-vykkyydet	Turvataan digitaalisen yhteiskunnan keskeiset tiedot, tietovarannot ja -palvelut	On tunnistettu tarve kartoittaa yhteiskunnan kriittiset tiedot ja palvelut, ja varmistaa näiden turvallisuus.	Tunnistetaan yhteiskunnan kannalta kriittiset tietovarannot, -palvelut ja -järjestelmät ja varmistetaan näiden toiminta sekä turvallisuus. Varmistetaan myös uusien, yhteiskunnan toiminnan kannalta kriittisten palveluiden turvallisuus osana niiden kehitystyötä. Näitä tehtäviä edistetään yhteistyössä Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelman 2020–2023 (Haukka) sekä Digitaalinen turvallisuus 2030 -hankkeen kanssa. Erillisselvityksen investointitarpeiksi arvioidaan 200 000 €.	Kansainvälinen	-	* Tunnistetaan yhteiskunnan kannalta kriittiset tietovarannot, -palvelut ja -järjestelmät ja varmistetaan näiden toiminta sekä turvallisuus. * Varmistetaan uusien, yhteiskunnan toiminnan kannalta kriittisten palveluiden turvallisuus osana niiden kehitystyötä.
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	Erittäin suuri	
					Organisaatio / Yritys	-	
					Kansalainen	Suuri	
12	Tehokkaat kansalliset kyberturvaky-vykkyydet	Kotimaisen salausteknologian luonti ja AQUA -statuksen saavuttaminen	Kotimaista salaustuoteperhettä tulee edelleen kehittää sekä mahdollistaa sen vienti myös kansainvälisille markkinoille. AQUA -statuksen puuttuminen ei edistä kansallisia salauskyvykkyyksiä, eikä uusia kasvun mahdollisuuksia.	Kansallista salaustuoteperhettä kehitetään edelleen. Rakennetaan AQUA-statuksen edellyttämät kyvykkyydet ja AQUA-status saavutetaan. Kotimaista salausteknologiaa hyödynnetään kansallisesti ja viedään kansainväliseen markkinaan. Kotimaisen salaustuoteperheen edelleen kehittäminen sekä AQUA statuksen saavuttaminen nähdään erittäin suurena mahdollisuutena. Tämä edellyttää myös krypto-strategiatyön vakiinnuttamista. Näiden vuosittaiset investointikustannuksen arvioidaan olevan 2 milj. € (salaustuoteperhe) + 1 milj. € (AQUA-status).	Kansainvälinen	Erittäin suuri	* Parannetaan kansallista salaustuoteperhettä. Vakiinnutetaan kryptostrategiatyö. * Rakennetaan AQUA-statuksen saavuttamiseksi vaadittavat kyvykkyydet. * Tunnistetaan kansallisesti kriittiset kyberturvayhtiöt ja turvataan niiden kotimaiset omistusosuudet.
					Kansallinen	Erittäin suuri	
					Hallinnonala / Toimiala	Erittäin suuri	
					Organisaatio / Yritys	Erittäin suuri	
					Kansalainen	Merkittävä	

Liite 3. Kehittämisohjelman laadinnassa huomioituja muita strategioita, hankkeita ja selvityksiä

- **Osallistava ja osaava Suomi – sosiaalisesti, taloudellisesti ja ekologisesti kestävä yhteiskunta**, Pääministeri Sanna Marinin hallitusohjelma 2019

- **Valtioneuvoston periaatepäätös Suomen kyberturvallisuusstrategia 2019:** Periaatepäätöksen kolme strategista linjausta ovat kansainvälinen yhteistyö, kyberturvallisuuden johtamisen, suunnittelun ja varautumisen parempi koordinaatio sekä kyberturvallisuuden osaamisen kehittäminen. Kyberturvallisuuden voimavarojen kohdentamista ja yhteistoimintaa parantaa hallituskausien yli ulottuva kyberturvallisuuden kehittämisohjelma. Ohjelma konkretisoi kansallisia linjauksia sekä selkiyttää hankkeiden, tutkimuksen ja kehittämisohjelmien kokonaiskuvaa. Kyberturvallisuuden kansallista kehittämistä koordinoimaan perustetaan liikenne- ja viestintäministeriöön kyberturvallisuusjohtajan tehtävä.

- **Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla.** Liikenne- ja viestintäministeriö 2021.

- **European Union Agency for Cybersecurity (ENISA), 'Trusted and cyber secure Europe':** ENISA:n strategian tavoitteena on mm. saavuttaa korkea kyberturvallisuuden taso jäsenmaissa yhteistyössä eri maiden ja toimijoiden kanssa. Edelleen strategian tavoitteena on rakentaa luottamusta verkottuneeseen yhteiskuntaan ja sen palveluihin, nostaa resilienssiä, sekä näin varmistaa sekä jäsenvaltioiden että niiden kansalaisten turvallisuus.

- **Valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta:** Valtioneuvoston periaatepäätös julkisen hallinnon digitaalisesta turvallisuudesta ja sen toimeenpano-ohjelma muodostaa keskeisen osan kyberturvallisuuden kehittämisohjelmaa. Tässä periaatepäätöksessä määritetään kehittämisen periaatteet ja keskeiset palvelut turvallisuuden edistämiseksi digitaalisessa toimintaympäristössä. Periaatepäätöksen tavoitteena on suojata kansalaisia, yhteisöjä ja yhteiskuntaa niiltä kokonaisturvallisuuden riskeiltä ja uhkilta, jotka voivat kohdistua tietoihin, palveluihin ja yhteiskunnan toimintaan digitaalisessa toimintaympäristössä.

- **Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka)**: Haukka-ohjelmassa kuvataan periaatepäätöksen toteuttaminen. Haukka-toimeenpanosuunnitelmaan on valittu 19 tehtävää, joiden avulla kehitetään keskeisiä julkisen hallinnon digitaalisen turvallisuuden palveluita. Toimeenpanosuunnitelmalla tuetaan myös käynnistymässä olevaa kyberturvallisuusstrategian 2019 kehittämisohjelman valmistelua ja toteuttamista, sekä osaltaan pannaan täytäntöön valtioneuvoston päätöstä huoltovarmuuden tavoitteista

- H**uoltovarmuuskeskuksen Digitaalinen Turvallisuus 2030 -ohjelma:** Ohjelmassa kehitetään yhteiskunnan digitaalisen infrastruktuurin ja sen palvelujen häiriönsietoisuutta ja kyberturvallisuutta yhteistyöprojekteissa yritysten ja verkostojen kanssa. Ohjelma täydentää osaltaan kehittämisohjelman sisältöä ja tavoitteita.

- **Valtioneuvoston puolustusselonteko, 2017.** Valtioneuvoston puolustusselonteko eduskunnalle antaa puolustuspoliittiset linjaukset Suomen puolustuskyvyn ylläpidolle, kehittämiselle ja käytölle. Puolustusselonteolla ja sen toimeenpanolla varmistetaan, että Suomen puolustuskyky vastaa turvallisuusympäristön vaatimuksiin.

- **Työ- ja elinkeinoministeriön Kasvua digitaalisesta turvallisuudesta – tiekartta 2019–2030:** Digitaalisen turvallisuuden kasvun tiekartan tavoitteena on edistää digitaaliseen turvallisuuteen ja osaamiseen liittyvää yritysvetoista kehitystä, kasvua ja kansainvälistymistä yritysten, julkisen sektorin ja tutkimuslaitosten yhteistyönä. Raportissa esitetään digitaalisen turvallisuuden alan yhteinen tavoitetila ja tulevaisuuskuva vuodelle 2030, kuvataan alan osaaminen ja toimintaympäristö, määritetään teemakohtaiset visiot vuodelle 2030 ja keskeiset välitavoitteet vuosille 2021 ja 2025.

- **Teknologian tutkimuskeskus VTT Oy:n tutkimus 'Current Level of Cybersecurity Competence and Future Development – Case Finland'** kuvaa suomalaisen kyberturvallisuusosaamisen tilaa ja tulevaisuuden kehitystarpeita.

- **Kansainvälinen oikeus kybertoimintaympäristössä – oikeudellisia kantoja.** Ulkoministeriö 2020.

- **Kyberpuolustuksen kehittämisen strategiset linjaukset.** Puolustusministeriö 2019.

- **Kyberturvallisuuden sanasto.** Turvallisuuskomitea 2018.

Liite 4. Valmisteluryhmä

Kyberturvallisuuden kehittämisohjelman valmisteluryhmässä olivat mukana:

- kyberturvallisuusjohtaja *Rauli Paananen,* liikenne- ja viestintäministeriö, puheenjohtaja
- tietohallintoneuvos *Tuija Kuusisto,* valtiovarainministeriö
- tietohallintojohtaja *Ari Uusikartano*, ulkoministeriö
- lainsäädäntöneuvos *Tiina Ferm,* sisäministeriö
- tietohallintojohtaja *Mikko Soikkeli,* puolustusministeriö
- neuvotteleva virkamies *Pentti Olin,* puolustusministeriö
- pääsihteeri *Petri Toivonen*, Turvallisuuskomitea
- kenraalimajuri, johtamisjärjestelmäpäällikkö *Mikko Heiskanen,* Puolustusvoimat
- insinöörieversti *Janne Jokinen,* Puolustusvoimat
- Suojelupoliisin edustaja
- työelämäprofessori *Martti Lehto,* Jyväskylän yliopisto
- professori *Juha Röning,* Oulun yliopisto
- toiminnanjohtaja *Mika Susi,* Kyberala Ry
- liiketoimintajohtaja *Anssi Kärkkäinen,* Cinia Oy
- yhteiskuntasuhdejohtaja *Nina Hyvärinen,* F-Secure
- toimitusjohtaja *Petri Kairinen,* Nixu Oyj
- turvallisuusjohtaja *Jari Pirhonen,* TietoEVRY Oyj

Twitter: @lvm.fi
Instagram: lvmfi
Facebook.com/lvmfi
Youtube.com/lvm.fi
LinkedIn: Liikenne- ja viestintäministeriö

lvm.fi

LIIKENNE- JA VIESTINTÄMINISTERIÖ

ISSN 1795-4045
ISBN 978-952-243-599-6