Liitteet

Liite 1: Kehittämisohjelman toimeenpanosuunnitelma

Liite 2: Kehittämistoimenpiteiden vaikuttavuusanalyysi

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

Liite 1: Kehittämisohjelman toimeenpanosuunnitelma

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 toiminta-menot	Päivä on toteutettu.
1.2	Huippuluokan osaaminen	Järjestöjen roolin määrittely kansallisessa kyberturvallisuuden valistustyössä ja tämän tehtävän tukeminen	LVM, PLM, TK-sihteeristö	2021	Normaalit toiminta-menot	Järjestöillä on selkeä rooli valistustyössä. 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 kiinnostumaan kyberalasta.	LVM, TEM, SM, TK-sihteeristö, Kyberala (FISC)	2021-2024	Normaalit toiminta-menot	Nykytila ja tarvittavat kehittämistoimenpiteet on tunnistettu. Kehittämistoimenpiteitä on toteutettu. Opintoihin on hakeutunut ja alalle on työllistetty nykyistä enemmän naisia.
1.5	Huippuluokan osaaminen	Järjestöjä tuetaan vakavien kyberhyökkäystilanteiden jälkihoitoon liittyvissä valmiuksissa sekä näiden toteutuksessa yhteistyössä viranomaisten kanssa.	LVM, PLM, TK-sihteeristö	2021	Normaalit toiminta-menot	Toimintamalli on määritelty Valmiudet luotu.
1.6	Huippuluokan osaaminen	Kansalaisille kohdistetun kyberturvallisuustietoisuuden viestintäsuunitelman laatiminen.	LVM, VM, TK-sihteeristö	2021	Normaalit toiminta-menot	Kansalaisten kyberturvallisuus tietoisuuden kasvattamiseen tähtäävä viestintäsuunnitelma on luotu ja sen mukainen toiminta on käynnistynyt.
2	**Kyberturvallisuuden koulutusjärjestelmän kehittäminen**					
2.1	Huippuluokan osaaminen	Koulutusjärjestelmän muutostarpeiden tunnistaminen	LVM, TEM, OKM	Selvitetään aikataulu	450 000 €/tutkimus	Kyberturvallisuuden koulutukseen liittyvät

		yhteistyössä korkeakoulujen kanssa.				muutostarpeet on tunnistettu.
2.2	Huippuluokan osaaminen	Varhaiskasvatuksessa luodaan perusteet lapsille ymmärtää, kuinka käyttää turvallisesti digitaalisen yhteiskunnan tuotteita ja palveluita.	OKM	Selvitetään aikataulu	Normaalit toiminta-menot	Kyberturvaopinnot sisällytetty opetussuunnitelmaan.
2.3	Huippuluokan osaaminen	Kyberturvallisuus sisällytetään peruskoulun opetussuunnitelmaan.	OKM	Selvitetään aikataulu	Normaalit toiminta-menot	Kyberturvaopinnot sisällytetty opetussuunnitelmaan.
2.4	Huippuluokan osaaminen	Lukiokoulutuksessa laajennetaan ja syvennetään em. taitoja ja luodaan perustaa alan erityisosaamiselle korkea-asteen koulutuksessa.	OKM	Selvitetään aikataulu	Normaalit toiminta-menot	Kyberturvallisuus opinnot sisällytetty opetussuunnitelmaan.
2.5	Huippuluokan osaaminen	Ammatilliseen koulutukseen sisällytetään kyberturvallisuuden alan perusammattitaitoon tähtäävät opinnot.	OKM	Selvitetään aikataulu	Normaalit toiminta-menot	Kyberturvaopinnot sisällytetty opetussuunnitelmaan.
2.6	Huippuluokan osaaminen	Ammatillisen ja täydentävän kyberturvaosaamisen kehittämiseksi suunnitellaan osaamispolkuja, joissa hyödynnetään olemassa olevia ja luodaan tarvittaessa uusia sisältöjä.	OKM	Selvitetään aikataulu	Normaalit toiminta-menot	Kyberturvallisuuden opintopolkuja luotu ja niitä toteutetaan.
2.7	Huippuluokan osaaminen	Huippu- ja erityisosaamistarpeet tunnistetaan ja osaamista kehitetään tarpeiden mukaisesti.	OKM, LVM, TEM, Kyberala (FISC), PLM, SM	Selvitetään aikataulu	Normaalit toiminta-menot	Tarpeet on tunnistettu ja osaamisen kehittäminen on mahdollistettu.
2.8	Huippuluokan osaaminen	Yhteisiä kyberturvakoulutuksia järjestetään keskitetysti.	LVM, PLM, SM	Selvitetään aikataulu	600 000 €/v	Yhteisiä koulutuksia on järjestetty.
2.9	Huippuluokan osaaminen	Toteutetaan jo tunnistetut keinot, ml. lupaprosessin sujuvoittaminen, nopeuttamaan ja helpottamaan kansainvälisten kyberturvallisuusammattilaisten rekrytointia suomalaisen teollisuuden palvelukseen sekä huippuosaajia alan tutkimus- ja opetustyöhön	SM, TEM, Kyberala (FISC)	2021-2025	Normaalit toiminta-menot	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 toiminta-menot	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.

4	**Kansallisen kyberturvallisuuden tutkimus- ja kehitysyhteistyön edistäminen**					
4.1	Kiinteä yhteistyö	Kyberturvallisuuden tutkimus- ja kehitysyhteistyötä 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 €/suunnitte-lutyö	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 toiminta-menot	Kaupallistamiseen johtavia tutkimustuloksia on syntynyt.
5	**Aktiivinen osallistuminen ja vaikuttaminen kansalliseen ja kansainväliseen kyberturvallisuuden yhteistyöhön**					
5.1	Kiinteä yhteistyö	Osallistutaan aktiivisesti kansainväliseen kyberturvayhteistyöhön. Kyberturvateollisuudelle luodaan mahdollisuudet osallistua yhteinen kannan valmistemuun 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.

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.
6.8	Vahva kotimainen kyberturvateollisuus	Perustetaan kyberturvallisuuden kasvu- ja osaamiskeskus	TEM, Kyberala (FISC), Kansallinen koordinaatiokeskus	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 koordinaatiokeskus	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, VM, VNK, LVM, Kyberala (FISC), Kansallinen koordinaatiokeskus	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.
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	Arvioidaan viranomaisten toimintaedellytykset nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa ottaen huomioon uhkaympäristön jatkuva kehittyminen sekä käynnistetään tarvittavat toimet.	PLM, SM, LVM, UM	2021-2023	Täydennetään selvitystyön valmistuttua.	Arviointityö on tehty ja kehittämistarpeet on tunnistettu ja niitä on toteutettu.
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 kyberturva-kyvykkyydet	Määritellään huoltovarmuuskriittisten sektoreiden ml. yritykset kyberturvallisuusvaatimuksille yhteinen vähimmäistaso.	HVK, kaikki ministeriöt	2021	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, sektorikohtaiset NIS -viranomaiset	Jatkuva	Normaalit toimintamenot	Toimialakohaisten valvovien viranomaisten tilannekuvakyvykkyyksille on asetettu yhteinen tavoite, kyvykkyydet tunnistettu, toimintaa on kehitetty ja jatkuva toiminta on käynnissä.
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.
12	**Kotimaisen salausteknologian luonti ja AQUA -statuksen saavuttaminen**					
12.1	Tehokkaat kansalliset kyberturvakyvykkyydet	Parannetaan kansallista salaustuoteperhettä sekä vakiinnutetaan krypto-strategiatyö	Kyberala (FISC), LVM, PV	2021-2027	2 milj. €/v	Kansallinen salaustuoteperhe on valmis.
12.2	Tehokkaat kansalliset kyberturvakyvykkyydet	Rakennetaan AQUA-statuksen saavuttamiseksi vaadittavat kyvykkyydet.	LVM, Traficom, VTT	2021-2027	1 milj. €/v	Vaadittavat kyvykkyydet on rakennettu.
12.3	Tehokkaat kansalliset kyberturvakyvykkyydet	Tunnistetaan kansallisen turvallisuuden näkökulmasta kriittiset kyberturvallisuusyhtiöt ja turvataan niiden kansalliset omistusosuudet.	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**	**Kehittämisohjelman 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** **Kansallinen** **Hallinnonala / Toimiala** **Organisaatio / Yritys** **Kansalainen**	**Suuri** **Erittäin suuri** **Suuri** **Erittäin suuri** **Erittäin suuri**	* Kyberturvapäivän toteuttaminen osana digiturvaviikkoa. * Järjestöjen roolin määrittely kansallisessa kyberturvallisuuden valistustyössä 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.
2	**Huippuluokan osaaminen**	**Kyberturvallisuuden koulutusjärjestelmän kehittäminen**	Koulutusjärjestelmään ei ole sisällytetty riittävästi elinkeinoelämän ja yhteiskunnan tarpeita tukevia kyberturvallisuuden opintoja. Koulutusjärjestelmä ei nykytilassa valmista asiantuntijoita em. tarpeisiin ja asiantuntijat koulutetaan vasta työelämään astumisen jälkeen.	Koulutusjärjestelmän sisällöt ja oppimispolut olisi suunniteltu siten, että koulutusjärjestelmä tuottaisi 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.	**Kansainvälinen** **Kansallinen** **Hallinnonala / Toimiala** **Organisaatio / Yritys** **Kansalainen**	**Suuri** **Erittäin suuri** **Erittäin suuri** **Erittäin suuri** **Merkittävä**	* Varhaiskasvatuksessa luodaan perusteet lapsille ymmärtää, kuinka käyttää turvallisesti digitaalisen yhteiskunnan tuotteita ja palveluita. * Kyberturvallisuus sisällytetään peruskoulun opetussuunnitelmaan * Lukiokoulutuksessa laajennetaan ja syvennetään em. taitoja ja luodaan perustaa alan erityisosaamiselle korkea-asteen koulutuksessa. * Ammatilliseen koulutukseen sisällytetään kyberturvallisuuden alan perusammattitaitoon tähtäävät opinnot. * Ammatillisen ja täydentävän kyberturvaosaamisen kehittämiseksi suunnitellaan osaamispolkuja, joissa hyödynnetään olemassa olevia ja luodaan tarvittaessa uusia sisältöjä. * Huippu- ja erityisosaamistarpeet tunnistetaan ja osaamista kehitetään tarpeiden mukaisesti. * Yhteisiä kyberturvakoulutuksia järjestetään keskitetysti

				Edelleen kyberturvallisuuden koulutuksien nykyistä tiiviimpi keskittäminen luo parempia mahdollisuuksia osaamisen jatkuvaan kehittämiseen sekä toteuttamiseen kansallisesti. Tämän toteuttamiseen arvioidut investoinnit ovat vuositasolla 600 000 €.			
3	**Kiinteä yhteistyö**	**Kyberturvallisuuden harjoitustoiminnan 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** **Kansallinen** **Hallinnonala / Toimiala** **Organisaatio / Yritys** **Kansalainen**	**-** **Erittäin suuri** **Suuri** **Suuri** **-**	* Yhteistyö viranomaisten, elinkeinoelämän ja järjestöjen välillä kriittisten arvoketjun turvaamiseen liittyvässä harjoitustoiminnassa. * Yhteisten kyberharjoitusympäristöjen hyödyntäminen ja niiden toiminnan varmistaminen.
4	**Kiinteä yhteistyö**	**Kansallisen kyberturvallisuuden tutkimus- ja kehitysyhteistyön edistäminen**	Kyberturvallisuuden tutkimusta tehdään, mutta sitä ei koordinoida yhteisten tavoitteiden saavuttamiseksi. Tutkimustulosten kaupallistamisessa on haasteita. Tutkimusrahoitusta ei ole saatavilla riittävästi.	Kyberturvallisuuden tutkimus- ja kehitysyhteistyötä 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 kehitystyön rooli nähdään erittäin merkittävänä. Tutkimus luo potentiaalia uusille innovaatioille sekä kasvulle. Tälle työlle on arvioitu vuosittaiseksi investointitarpeeksi 1 milj. €.	**Kansainvälinen** **Kansallinen** **Hallinnonala / Toimiala** **Organisaatio / Yritys** **Kansalainen**	**-** **Erittäin suuri** **Erittäin suuri** **Suuri** **-**	* Kyberturvallisuuden tutkimus- ja kehitysyhteistyötä 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.

				Eri yhteisöjen aktivoinnissa nähdään merkittäviä mahdollisuuksia myös digitalisen yhteiskunnan kyberturvallisuuden kehittämisessä. Yhteisön aktivointi vaatii yhteiset pelisäännöt ja toimintamallit. Niiden toteuttamisen investointitarpeiksi arvioidaan 100 000 €.			
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** **Kansallinen** **Hallinnonala / Toimiala** **Organisaatio / Yritys** **Kansalainen**	**Erittäin suuri** **Erittäin suuri** **-** **Merkittävä** **-**	* Osallistutaan aktiivisesti kansainväliseen kyberturvayhteistyöhön * Suomen menestymistä kansainvälisellä kyberturvakentällä seurataan kansainvälisiin indekseihin perustuen
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** **Kansallinen** **Hallinnonala / Toimiala** **Organisaatio / Yritys** **Kansalainen**	**Erittäin suuri** **Erittäin suuri** **Suuri** **Erittäin suuri** **Merkittävä**	*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.
7	**Vahva kotimainen kyberturvateollisuus**	**Uusien kyberturvayritysten perustamisen edistäminen**	Uusien kyberturvayritysten perustamiseen liittyvää tukea tulee edelleen kehittää tuotteistamisen, rahoitukset että elinkaaren eri vaiheissa olevien yritysten tukemisen.	Kyberturvateollisuudelle on tarjolla riittävästi pääomia ja rahoitusta. Elinkaaren eri vaiheissa olevien yritysten toimintaa tuetaan sopivin tavoin.	**Kansainvälinen** **Kansallinen** **Hallinnonala / Toimiala** **Organisaatio / Yritys**	**-** **Suuri** **Suuri** **Erittäin suuri**	* 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-

					Kansalainen	**Merkittävä**	hankkeen kanssa huomioiden TKI-hankinnat. * Käynnistetään pilottihanke kyberturvallisuuden osa-alueella yhteistyössä työ- ja elinkeinoministeriön KEINO-hankkeen ja vaikuttavuusinvestoimisen osaamiskeskuksien kanssa
8	**Tehokkaat kansalliset kyberturvakyvykkyydet**	**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 arvioitu. Arvioinnissa huomioidaan riskit sekä laaja-alaisesti käytössä olevat riskienhallintakeinot ja kyvykkyydet sekä tunnistetaan tarvittavat kehittämistoimet ja niitä on käynnistetty. 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. Investointitarpeet tarkentuvat selvitystyön valmistuttua.	**Kansainvälinen**	**-**	* Arvioidaan viranomaisten toimintaedellytykset nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa ottaen huomioon uhkaympäristön jatkuva kehittyminen.
					Kansallinen	**Erittäin suuri**	
					Hallinnonala / Toimiala	**Erittäin suuri**	
					Organisaatio / Yritys	**Suuri**	
					Kansalainen	**-**	
9	**Tehokkaat kansalliset kyberturvakyvykkyydet**	**Kehitetään kansallisten verkkopalveluiden sisäänrakennettua 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 kyberturvakyvykkyydet**	**Harmonisoidaan turvallisuusvaatimuksia ja parannetaan havainnointikykyä**	Huoltovarmuuskriittisten sektoreiden turvallisuusvaatimukset eroavat toisistaan. Tarve havainnointikyvyn ja tilannekuvan muodostamiseen liittyvien kyvykkyyksien kehittämiseen on tunnistettu.	Huoltovarmuuskriittisten sektoreiden turvallisuusvaatimukset on kartoitettu ja varmistettu, että niillä saavutetaan riittävä turvallisuuden taso. Operatiivisen tilannekuvan muodostamiseen liittyvät kyvykkyydet on olemassa, siten	**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
					Kansallinen	**Erittäin suuri**	
					Hallinnonala / Toimiala	**Erittäin suuri**	
					Organisaatio / Yritys	**-**	
					Kansalainen	**-**	

				että kansallinen, kyberturvallisuuden tilannekuva voidaan muodostaa.			valvovien viranomaisten tilannekuvan tuottamiseen liittyviä kyvykkyyksiä kansallisen kyberturvallisuuden tilannekuvan parantamiseksi
11	**Tehokkaat kansalliset kyberturvakyvykkyydet**	**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 kyberturvakyvykkyydet**	**Kotimaisen salaustuoteperheen parantaminen 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.

- **Selvitys tietoturvan ja tietosuojan parantamiseksi kriittisillä toimialoilla.** Liikenne- ja viestintäministeriö 2021.

- **European Union Agency for Cybersecurity (ENISA), 'Trusted and cyber secure Europe':** ENISAn 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

- **Huoltovarmuuskeskuksen 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.