VALTIONEUVOSTO
STATSRÅDET

Kyberturvallisuusstrategian toimeenpanosuunnitelma

3.12.2024 - VN/36693/2023

Sisällysluettelo

1. Johdanto

Suomen kyberturvallisuusstrategia 2024-2035 on hyväksytty valtioneuvoston periaatepäätöksenä 10.10.2024. Sen toimeenpanosuunnitelma kuvaa tavoitteiden saavuttamiseksi tarvittavat toimenpiteet vastuineen ja mittareineen. Toimeenpanosuunnitelma hyväksyttiin valtiosihteereistä koostuvassa valtioneuvoston turvallisuusjohtamisen toimintamallin kehittäminen -hankkeen ohjausryhmässä 3.12.2024.

Strategian ja sen toimeenpanosuunnitelman laatimiseen ovat osallistuneet sadat asiantuntijat, julkisen ja yksityisen sektorin, tiedeyhteisön sekä kansalaisjärjestöjen toimijat. Tämä kuvastaa suomalaisen yhteiskunnan sitoutumista ja suomalaista kokonaisturvallisuuden mallia.

Toimeenpanosuunnitelma sisältää toimenpiteet kyberturvallisuusstrategian tavoitteiden saavuttamiseksi. Suunnitelman toteuttaminen sidotaan julkisen talouden suunnitteluprosessiin. Toimeenpanosuunnitelmaa seurataan vuosittain ja päivitetään tarvittaessa. Valtiosihteerien ohjausryhmä seuraa strategian toteutusta vuosittain.

Kyberturvallisuusjohtajan toimistolla on seurannan koordinoinnin päävastuu, ja ministeriöistä koostuva seurantaryhmä ja sen sihteeristö tukevat toimistoa seurannassa. Jokainen hallinnonala vastaa niille nimettyjen toimenpiteiden edistämisestä, rahoituksesta ja raportoinnista. Toimeenpanosuunnitelmaa on mahdollista päivittää vuosittain.

Toimeenpanosuunnitelman kokonaisvaikuttavuutta arvioidaan erilaisilla mittareilla, kuten kyberturvallisuuden kansallisilla ja kansainvälisillä suorituskykyindikaattoreilla.

2. Kyberturvallisuusstrategian tavoitetila ja strategian rakenne

3. Yhteiskunnan toimijat kansallisen kyberturvallisuuden varmistamisessa

Yhteiskunnan toimijat kansallisen kyberturvallisuuden varmistamisessa

4. Toimeenpanosuunnitelman rakenne

Toimeenpanosuunnitelma ulottuu vuoteen 2035, ja se kattaa kaikki yllä mainitut neljä osa-aluetta eli pilaria:

I Osaaminen, teknologia ja tutkimus-, kehitys- ja innovaatiotoiminta (TKI);
II Varautuminen;
III Yhteistoiminta;
IV Reagointi ja vastatoimet.

Toimeenpanosuunnitelman rakenne on kytketty näiden neljän pilarin sisältämiin strategisiin tavoitteisiin ja kehittämisehdotuksiin. Nämä puolestaan on johdettu strategiassa määritellystä kansallisen kyberturvallisuuden tavoitetilasta.

Suunnitelman toimenpiteet on priorisoitu kahteen luokkaan eli ”koriin”:
Kori 1 tarkoittaa strategisia kärkihankkeita, joiden vaikuttavuus on suuri tai erittäin suuri ja jotka pyritään toteuttamaan ensin.
Kori 2 sisältää pidemmällä aikavälillä toteutettavia hankkeita, joiden vaikuttavuutta ei tällä hetkellä ole arvioitu yhtä kriittiseksi.

Jokaisesta toimenpiteestä kuvataan sen tavoitteet, aikataulu ja rahoitus, vaikuttavuus sekä toimenpiteen toteuttamiseen osallistuvat toimijat (**pääasiallinen vastuutaho** ja muut toimijat). Kunkin toimenpiteen vaikuttavuutta arvioidaan sanallisella vaikuttavuusarviolla sekä asteikoilla kansallinen/kansainvälinen sekä merkittävä/suuri/erittäin suuri.

5. Toimeenpanosuunnitelman toteuttaminen ja seuranta

Seurannan koordinointivastuu on valtion kyberturvallisuusjohtajan toimistolla, jolle hallinnonalat tuottavat kyberturvallisuuden toimeenpanoraportin omasta vastuualueestaan julkisen talouden suunnitteluprosessin aikataulun mukaisesti. Näistä toimisto laatii koosteen viranomaisille ja poliittisille päättäjille.

Valtioneuvoston kanslia on 1.11.2024 asettanut seurantaryhmän, joka vastaa kyberturvallisuusstrategian toimeenpanon seurannasta ja vaikutusten arvioinnista. Seurantaryhmä kokoontuu noin neljännesvuosittain tai tarvittaessa useamminkin.

Sidosryhmillä on mahdollisuus osallistua strategian toimeenpanosuunnitelman seurantaan. Sidosryhmiä kuullaan kootusti keväisin, ja vuoropuhelua käydään aktiivisesti pitkin vuotta.

Hallinnonalat suunnittelevat ja varaavat toimeenpanon edellyttämät resurssit ja vastaavat kehittämistoimien toimeenpanosta.

Seurannassa tarkastellaan, miten eri toimenpiteet ovat toteutuneet verrattuna strategian tavoitetilaan ja strategiassa määriteltyihin kehittämisehdotuksiin. Raportoinnissa keskitytään erityisesti siihen, mitä menneen kauden aikana on saatu aikaan ja missä vielä on kehitettävää. Painopiste on konkreettisten tulosten raportoinnissa, ja tärkeää on kertoa myös, miksi jotakin toimenpidettä ei ole tehty.

5. Seurannan toteuttaminen; vastuut

Valtiosihteerien ohjausryhmä (TUJO)	• Hyväksyy toimeenpanosuunnitelman • Seuraa toimeenpanosuunnitelman toteutusta vuosittain (seurantaraportti)
Valtion kyberturvallisuusjohtajan toimisto Sihteeristö	• Seurannan koordinointivastuu • Järjestää seurantaryhmän kokoukset • Järjestää vuosittain yhteisen tilaisuuden toimeenpanosuunnitelman edistymisestä sidosryhmien kanssa • Laatii seurantaraportin seurantaryhmän vastausten pohjalta • Vastaa raportoinnista VSI OHRY, YU minry, TK (+ tarvittaessa muut tahot) • Seurantaryhmän sihteeristö toimii KTJ-toimiston tukena seurannassa
Kyberturvallisuusstrategian seurantaryhmä	• Laatii, yhteensovittaa ja tarvittaessa päivittää toimeenpanosuunnitelman • Muodostaa kokonaisnäkemyksen hallinnonalojen vastauksista • Toimittaa edistymistiedot seurantaraporttiin
Vastuuhallinnonala/ muu toimija	• Suunnittelee ja varaa resurssit • Kehittää oman vastuualueensa osalta tarvittavat yhteistyörakenteet • Toimeenpanee kehittämistoimen joko päävastuussa tai osallistuvana • Raportoi hallinnonalallaan, sektorillaan ja seurantaryhmälle

VALTIONEUVOSTO
STATSRÅDET

Toimeenpanosuunnitelma; toimenpiteet

Pilari I: Osaaminen, teknologia ja TKI ”Osaava, innovatiivinen ja kokeileva kyberekosysteemi”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
1.1.	**Kehitetään julkisen ja yksityisen sektorin huippuosaamista ja työelämätaitoja sekä kansalaisten ja kansalaisyhteiskunnan kybervalmiuksia ja varautumista** **Kori 1**	• Kehitetään kyberturvallisuuden osaamista kaikilla koulutusasteilla, vapaassa sivistystyössä, työvoimakoulutuksissa ja täydennyskoulutuksissa. • Kasvatetaan työelämän kyberturvallisuustaitoja edistävien koulutusten vaikuttavuutta ja saatavuutta. • Parannetaan kansalaisten valmiuksia toimia turvallisesti. • Varmistetaan Cyber Citizen -hankkeen tulosten hyödyntäminen ja rahoitus. • Luodaan edellytykset huippuosaamisen kasvattamiselle kyberalan TKI-toiminnan kautta. • Kasvatetaan turvallisen ohjelmistokehityksen osaamista ja saatavuutta. • Hyödynnetään Puolustusvoimien ja sidosryhmien kyberkoulutusta kansallisen osaamisen lisäämisessä. • Kehitetään vapaaehtoisen maanpuolustuksen hyödyntämistä.	2025 alkaen Toiminta-menot, osin lisäresurssit	Kyberturvallisuusosaamisen parantaminen yhteiskunnassa luo edellytykset yhteiskunnan toimivuudelle. Osaamista on parannettu kolmella tasolla: • kansalaistaidot, mukaan lukien varautuminen, • yleiset työelämätaidot, • huippuosaaminen. Koulutuksissa on huomioitu sekä osaamistarpeet että toimintaympäristön muutos ja teknologian murros. Vaikuttavuus: kansallinen/suuri.	**OKM, LVM, PLM, VNK, HVK,** Traficom, PV, MPK, HAUS, koulutus-järjes-telmän toimijat, elin-keino-elämä

Pilari I: Osaaminen, teknologia ja TKI ”Osaava, innovatiivinen ja kokeileva kyberekosysteemi”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
1.2.	**Kehitetään kyberturvallisuuden koulutuksen verkostoyhteistyötä** **Kori 1**	• Selvitetään verkostoyhteistyön laajentaminen ammatilliseen koulutukseen sekä yhteistyöhön muiden alan toimijoiden kanssa nykyisten Jyväskylän yliopiston ja ammattikorkeakoulun vetämien korkeakoulujen kyberosaamisen verkostojen pohjalta.	2026-2027 Lisä-resurssit	Koulutustoimijoiden yhteistyön parantaminen. Vaikuttavuus: kansallinen/suuri.	**OKM**

Pilari I: Osaaminen, teknologia ja TKI ”Osaava, innovatiivinen ja kokeileva kyberekosysteemi”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
1.3.	**Kehitetään kansallista salausteknologista kyvykkyyttä ja hankitaan kansainvälisiä tietoturvahyväksyntöjä myöntävän maan asema EU:ssa ja Naton salaustuotteita tuottavan maan status** **Kori 1**	• Luodaan kansallinen salausteknologinen strategia, toimeenpano-ohjelma ja hallintamalli. • Kehitetään kansainvälisesti yhteensopiva kansallinen salausteknologian viitearkkitehtuuri ja kvanttiturvallinen kansallinen salaustuoteperhe. • Rakennetaan kansallinen salausteknologinen laboratorio. • Kehitetään kansallisten salausratkaisuiden huoltovarmuutta. • Tuetaan salaustuotteiden vientiä. • Luodaan/laajennetaan kansallista salausteknologian koulutusohjelmaa ja muuta osaamisen kehittämistä.	2025-2035 Lisä-resurssit	Kriittisten salausteknologioiden omavaraisuus ja huoltovarmuus. Huoltovarmuuskriittisten toimijoiden kyky turvata oma toiminta salausteknologisilta uhkilta. Vienninedistäminen tukee omavaraisuutta ja huoltovarmuutta. Kyky suojata kriittiset kansalliset tietovarannot kvanttiaikakaudella. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**PLM**, TEM, LVM, Traficom, PV, HVK, BF, Tesi, VTT, teollisuus, korkea-koulut

Pilari I: Osaaminen, teknologia ja TKI ”Osaava, innovatiivinen ja kokeileva kyberekosysteemi”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
1.4.	**Otetaan kansallisesti käyttöön kvanttiturvalliset salausratkaisut** **Kori 1**	• Laaditaan suunnitelma ja ohjeistus kvanttiturvallisiin algoritmeihin siirtymiseksi huomioiden kansallisen kvanttistrategian linjaukset. • Tuetaan kriittisiä aloja kvanttisiirtymässä. • Arvioidaan tarvetta luoda velvoitteita kvanttikestävän salauksen käytölle. • Hyödynnetään innovatiivista julkisen hankinnan mallia.	2025-2035 Lisä-resurssit	Oikea-aikaisella siirtymällä kvanttiturvallisiin salausratkaisuihin estetään luottamuksellisten tietojen vaarantuminen tai kansallisesti suojattavien tietoaineistojen pääsy vääriin käsiin sekä varmistetaan järjestelmien ja palveluiden saatavuus. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM, TEM, VM**, **PLM**, PV, Traficom, Valtori, HVK

Pilari I: Osaaminen, teknologia ja TKI ”Osaava, innovatiivinen ja kokeileva kyberekosysteemi”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
1.5.	**Ennakoidaan ja seurataan uusien teknologioiden ja ilmiöiden vaikutuksia kyberturvallisuuteen** **Kori 1**	• Luodaan poikkihallinnollinen kyberturvallisuuden tulevaisuus- ja ennakointityömalli. • Tuotetaan analysoitua tietoa kyberturvallisuuden tulevaisuuden uhista ja mahdollisuuksista viranomaisten ja elinkeinoelämän käyttöön sekä hyödynnetään viranomaisten tilannekuvatoimintaa tiedon jakamisessa. • Käynnistetään viranomaisten ja elinkeinoelämän yhteistyönä kyberympäristön skenaariopohjainen tarkastelu.	2025 alkaen Toiminta-menot	Kyberturvallisuuden ilmiöiden ennakoinnilla voidaan tunnistaa tulevaisuuden sääntely-, resursointi- ja varautumistoimenpiteet sekä tukea toimialojen ja viranomaisten varautumista kyberuhkiin. Edellytys kansallisen uhka-arvion laatimiselle. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM, VNK,** muut ministeriöt, virastot, Traficom, HVK, elinkeinoelämä, tutkimuslaitokset

Pilari I: Osaaminen, teknologia ja TKI ”Osaava, innovatiivinen ja kokeileva kyberekosysteemi”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
1.6.	**Vahvistetaan suomalaisten organisaatioiden osallistumista kyberturvallisuuden rahoitusohjelmiin ja osaamisen verkostoyhteistyöhön** **Kori 2**	• Vaikutetaan EU:n rahoitusohjelmien työohjelmiin ja vahvistetaan suomalaisten yritysten, korkeakoulujen ja tutkimuslaitosten osallistumismahdollisuuksia rahoitusohjelmiin. • Varmistetaan riittävä vastinrahoitus hankkeisiin osallistumiseksi. • Edistetään kansallisten toimijoiden liittymistä osaksi EU:n kyberturvallisuuden osaamisyhteisöä ja vienninedistämisen mahdollisuuksia. • Ylläpidetään ja kehitetään kansallista koulutus- ja tutkimusyhteisöä ja tuetaan suomalaisia toimijoita löytämään kansallisia ja kansainvälisiä kumppaneita kansainvälisiin projekteihin. • Tuotetaan tilannekuvaa kyberturvallisuuden tutkimuksesta ja siihen saadusta rahoituksesta.	2025-2029 Lisä-resurssit	Toimenpiteellä voidaan edistää kansallisten kyberturvallisuuden innovaatioiden, tutkimuksen ja osaamisen kehittymistä. Parannetaan saatavilla olevan EU- ja Nato-rahoituksen hyödyntämistä kansallisesti ja luodaan kasvua kyberturvallisuuden alalle. Edistetään teknologista omavaraisuutta. Vahvistetaan kansallista kyberturvallisuuden ekosysteemiä ja ekosysteemin kansainvälistä kilpailukykyä, parannetaan alan liiketoiminta- ja vientimahdollisuuksia. Vaikuttavuus: kansallinen ja kansainvälinen / suuri.	**LVM, PLM**, **TEM**, **OKM**, **VNK,** UM, Traficom, HVK

Pilari I: Osaaminen, teknologia ja TKI ”Osaava, innovatiivinen ja kokeileva kyberekosysteemi”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
1.7.	**Kehitetään ja tuetaan kansallista puolustusteollisuutta puolustusteknologioiden, murrosteknologioiden ja kaksoiskäyttötuotteiden innovoinnissa, hyödyntämisessä sekä uhkiin varautumisessa** **Kori 1**	• Saatetaan loppuun ja tuotteistetaan muun muassa F35-hankkeen epäsuoran teollisen yhteistyön turvallisen kommunikaation projektit. • Vakiinnutetaan Naton DIANA-ohjelman kansallisten keskusten ja yrityskiihdyttämöiden toiminta. • Tehostetaan EU:n ja Naton kehittämisrahoituksen hyödyntämistä. • Kaksoiskäyttötuotteiden osalta hyödynnetään tehokkaasti siviilirahoitusta. • Laaditaan puolustus- ja turvallisuussektorin (PUTU) kybersuojaamisen strategiset linjaukset ja perustetaan kyberturvallisuuden yhteistyöverkosto (ISAC). • Kehitetään yhteiset palvelut ja vastekyvyt PUTU-sektorille. • Vahvistetaan kotimaista omistajuutta huoltovarmuuden kannalta kriittisissä kyberturvallisuusalan yrityksissä.	2025 alkaen Toiminta-menot, osin lisäresurssit	Toimenpiteiden vaikuttavuutta arvioidaan muun muassa seuraavien indikaattorien kautta: • kansallinen maaprofiili murrosteknologioissa, • kansallinen TKI-rahoituksen taso, • kotimaisten kriittisten kärkiteknologiaratkaisuiden käyttöaste, • omavaraisuus ja vaikutukset huoltovarmuuteen, • vientipotentiaalin kasvu ja vientiarvo, • kansainväliset vaatimukset täyttävien ratkaisuiden hyödyntäminen ulkomailla, • kansallisten ratkaisujen käyttöaste, • kansallinen vastinraha (määrä, aika), ja • PUTU-sektorin kybersuojan taso. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**PLM, TEM, PV, VTT,** BF, Tesi, teollisuus

Pilari I: Osaaminen, teknologia ja TKI ”Osaava, innovatiivinen ja kokeileva kyberekosysteemi”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
1.8.	**Kehitetään järjestöjen ja elinkeinoelämän kanssa kyberturvallisuus-osaamista** **Kori 1**	• Käynnistetään yhdessä elinkeinoelämän ja järjestöjen kanssa hanke, jolla edistetään kansalaisten kyberturvallisuustaitojen parantamista. • Parannetaan viranomaisten ja järjestökentän yhteistyötä kansalaisiin ja eri väestöryhmiin kohdistuviin uhkiin liittyvässä tiedonvaihdossa ja viestinnässä. • Tuetaan järjestöjen oman kyberkyvykkyyden kehittymistä. • Vahvistetaan Finnish Safer Internet Centren (FISIC) toimintaa.	2025-2027 Toiminta-menot, osin lisäresurssit	Kansalaisten kyvyt toimia yhteiskunnassa turvallisesti vahvistuvat. Suomalaisten alttius menettää rahoja huijauksiin vähenee ja luottamus digitaaliseen yhteiskuntaan vahvistuu. Järjestöjen ja elinkeinoelämän kautta viedään viranomaisviestiä kyberturvallisuudesta, jotta kansalaisten osaaminen vahvistuu. Kansalaiset osaavat varautua digitalisoituneen yhteiskunnan häiriötilanteisiin. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM, OKM,** Kavi, Traficom**,** HVK, elinkeino-elämä, järjestöt

Pilari I: Osaaminen, teknologia ja TKI ”Osaava, innovatiivinen ja kokeileva kyberekosysteemi”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
1.9.	**Kehitetään kyberrikostorjunnan koulutusta** **Kori 2**	• Kehitetään kyberrikostorjunnan koulutusta tietoverkkorikosten ja tietoverkkoavusteisten rikosten osalta. Kehittämiseen liittyy jo aiemmin alkanut Kyberosake–hanke sekä tietoverkkoavusteisten rikosten torjunnan osaamisen hanke (TVA) .	2024 alkaen Toiminta-menot	Osaamisen kehittämisen tarve on tunnistettu poliisissa ja muissa turvallisuusviranomaisissa. Poliisiammattikorkeakoulun tarjoamalla koulutuksella varmistetaan osaamisen riittävyys poliisissa, ja koulutuksella tuetaan myös muiden turvallisuusviranomaisten toimintaa. Poliisiammattikorkeakoulun järjestämille koulutuksiin voivat turvallisuusviranomaisten lisäksi osallistua myös mm. syyttäjät ja tuomarit. Vaikuttavuus: kansallinen/suuri.	**SM,** Poliisi-hallitus, Poliisi-ammatti-korkea-koulu

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
2.1.	**Laaditaan kansallinen kyberuhka-arvio varautumistyön tueksi** **Kori 1**	• Laaditaan skenaariotyön pohjalta säännöllisesti kansallisia kyberturvallisuuden uhka-arvioita viranomaisten, julkisen hallinnon ja elinkeinoelämän käyttöön. • Lisätään kansallisten uhka-arvioiden saatavuutta ja hyödynnettävyyttä.	2025 alkaen Toiminta-menot	Tilannetietoisuus kyberuhista ja kyberturvallisuuteen vaikuttavista ilmiöistä paranee. Parannetaan toimialojen varautumisen, riskienhallinnan ja kriittisyysluokittelun edellytyksiä. Vahvistetaan jaettua kyberturvallisuuden tilannekuvaa. Uhka-arvio tukee NIS2:n edellyttämän kansallisen kyberkriisinhallintasuunnitelman laatimista ja siinä on huomioitu CER-direktiivin vaatimukset. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM**, **VNK, SM, PLM**, Traficom, PV, Supo, muu julkinen hallinto, elinkeino-elämä, HVK

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
2.2.	**Yhteensovitetaan kyberpuolustus kokonais-maanpuolustukseen** **Kori 1**	• Tunnistetaan ja hallitaan kyberpuolustuksen liitynnät kokonaismaanpuolustukseen, resilienssitoimiin ja isäntämaatukeen. • Huomioidaan kyberkriisien hallinnassa sotilaallinen maanpuolustus ja sotilaallinen kriisi sekä kehitetään siviilisektorin varautumista ja vastetta näihin. • Integroidaan paikalliskyberpuolustus paikallis- ja aluetason toimintamalleihin ja varautumiseen. • Varmistetaan viranomaisten kyky tukea kriittisiä toimijoita. • Kehitetään kokonaismaanpuolustuksen resurssien seurantaa kyberpuolustuksen osalta.	2025-2032 Toiminta-menot, osin lisäresurssit	Mahdollistetaan oma ja liittolaisten operointi ja operaatioiden tuki. Tarvittavat vastejärjestelmät on käyttöönotettu sekä ajantasaiset varautumissuunnitelmat ja sopimukset on tehty. Hallintasuunnitelmassa on huomioitu sotilaallinen uhka ja voimankäyttö. Siviilisektorin viranomaisten ja toimijoiden resursoinnin seuranta, resursoinnin vajeiden riskien tunnistaminen ja hallinta osana kokonaismaanpuolustuksen ohjausta. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**PLM,** PV, muut hallinnon-alat, siviili-sektori

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
2.3.	**Huomioidaan kyberturvallisuus kansallisissa lainsäädäntöhankkeissa** **Kori 2**	• Päivitetään lainvalmistelun vaikutusarviointi-ohje.	2025-2027 Toiminta-menot	Kansallisessa lainsäädännössä huomioidaan kyberturvallisuusnäkökohdat ja vastataan toimintaympäristössä tapahtuviin muutoksiin. Ministeriöiden lainvalmisteluissa ja lainsäädännön vaikutusarvioinneissa huomioidaan kyberturvallisuusnäkökulmat. Vaikuttavuus: kansallinen/suuri.	**OM,** muut minis-teriöt

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
2.4.	**Suunnitellaan ja seurataan julkisen hallinnon kyberturvallisuus-resursseja pitkäjänteisesti** **Kori 2**	• Valtion, hyvinvointialueiden ja kuntien kyberturvallisuuden resurssien suunnittelu ja seuranta sekä riskiperustainen resurssien kohdentaminen. • Hyödynnetään muun muassa DVV:n digiturvan kokonaiskuvapalvelua.	2025-2030 Toiminta-menot	Julkisen hallinnon kyberturvallisuuden resurssien tilanne on tunnettava riittävässä määrin tarkoituksenmukaisten resurssien varmistamiseksi ja tehokkaaksi käyttämiseksi. Resurssien käyttö kyberturvallisuuden varmentamisessa ja kohdentumisessa tehostuu muun muassa tehtävien priorisoinnin sekä ohjeistuksien avulla. Vaikuttavuutta mitataan hyödyntämällä digiturvan kokonaiskuvapalvelua ja ohjeistuksen toimivuutta. Vaikuttavuus: kansallinen/suuri.	**Minis-teriöt**, DVV, muu julkinen hallinto

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
2.5.	**Varmistetaan yhdenmukainen kyberturvallisuuslain toimeenpano** **Kori 1**	• Vahvistetaan NIS2-valvovien viranomaisten sekä tietosuojavaltuutetun yhteistyötä ja yhteistoimintaa. • Parannetaan toimialoille suunnattua neuvontaa ja ohjeistusta kyberturvallisuuslain ja lain julkisen hallinnon tiedonhallinnasta toimeenpanoon. • Laaditaan kansallinen laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelma. • Parannetaan tietosuojavaltuutetun toimintaedellytyksiä.	2025-2029 Toiminta-menot, osin lisä-resurssit	NIS2 -direktiivi on keskeinen kyberturvallisuuden säädös, joka yhtenäistää kriittisten toimialojen kyberturvallisuusvaatimuksia ja kasvattaa kansallista resilienssiä. Valvovien viranomaisten yhteistyöllä voidaan yhdenmukaistaa menettelyjä sekä tehostaa resurssien käyttöä. Yhteisillä ohjeistuksilla voidaan parantaa ja tehostaa lain toimeenpanoa organisaatioissa. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM, OM** VM, Traficom, TSV, NIS2 valvovat viran-omaiset
2.6.	**Vaikutetaan aktiivisesti kyberturvallisuuden kansainvälisiin standardeihin** **Kori 2**	• Vaikutetaan laajasti kyberturvallisuuden standardointityöhön kansainvälisissä järjestöissä. • Otetaan voimassa olevat standardit käyttöön etupainoisesti. • Kehitetään yksityisen sektorin osallistamista kansainväliseen standardointiin.	2025 alkaen Toiminta-menot	Varmistetaan riittävä kansallisten näkökohtien huomiointi standardien valmistelussa. Yksityisellä sektorilla on valmius ja kyky soveltaa standardeja. Standardointityöhön osallistumista kyetään hyödyntämään TKI-toiminnassa. Vaikuttavuus: kansallinen ja kansainvälinen / suuri.	**LVM, PLM,** muut ministeriöt, Traficom, PV

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
2.7.	**Ajantasaistetaan tietojärjestelmien, palveluiden ja turvallisuuskriittisten tuotteiden vaatimustenmukaisuuden arviointia koskeva lainsäädäntö sekä kehitetään organisaatioiden toimintaan ja tietojärjestelmiin liittyvää arviointitoimintaa** **Kori 1**	• Parannetaan arvioinnin saatavuutta ja viranomaisyhteistyötä tarkistamalla viranomaisten arviointitehtäviä. • Parannetaan turvallisuuskriittisten tuotteiden valmistajien ja arviointilaitosten elinkeinotoiminnan edellytyksiä työryhmän loppuraportin mukaisesti. • Sujuvoitetaan arviointimenettelyjä riskiperustaisesti sekä selkeytetään ja täydennetään arviointiperusteita. • Kehitetään ja yhtenäistetään arviointikriteeristöjä ja niiden käyttöä tukevia ohjeita ja työkaluja sekä teknisiä ja automaattisia menetelmiä. • PV:n kyky ja toimivalta sen omien tietojärjestelmien ja salausratkaisujen kansalliseen ja kansainväliseen arviointiin ja hyväksyntöihin saavutetaan. • Kehitetään sertifiointia ja olennaisia vaatimuksia sote-sektorilla asiakastietolain perusteella.	2024-2027 Toiminta-menot, osin lisäresurssit	Säädösten ajantasaistaminen on välttämätöntä toteuttaa toimintaympäristön muutosten johdosta valtiovarainministeriön työryhmän ”Julkisen hallinnon tietojärjestelmien vaatimusten-mukaisuuden nykytila-arviossa 2024” kuvatulla tavalla. Puolustusvoimilla ja Valtorilla on kyvykkyys riippumattomaksi varmistettuun arviointitoimintaan, yksityisen sektorin kyvykkyyttä arvioida ja tukea arviointeja on kehitetty. Turvallisuuskriittisen alojen tietojärjestelmien arviointia ja hyväksyntää tukeva infrastruktuuri rakennettu. Resursointitarve tarkentuu säädösvalmistelun yhteydessä. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**VM, LVM, PLM, STM,** muut ministeriöt, PV, KTJ, Traficom, Valtori, hyväksytyt arviointi-laitokset, muut arviointi-viran-omaiset, muu julkinen hallinto

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
2.8.	**Kehitetään kyberturvallisuus-harjoituksia vastaamaan muuttunutta toimintaympäristöä yhteiskunnan resilienssin kasvattamiseksi ja kokonais-maanpuolustuksen toimintaedellytysten turvaamiseksi** **Kori 1**	• Turvataan kansallisten kyberturvallisuusharjoitusten (KYHA) jatkuvuus. • Monipuolistetaan kansallista kyberharjoitustoimintaa ja kasvatetaan harjoitusten osallistujamääriä. • Kansallinen kyberharjoitustoiminta vastaa kokonaismaanpuolustuksen tarpeisiin. • Päivitetään harjoitusten skenaarioita. • Kehitetään sektori- ja toimialakohtaisia ja toimialojen välisiä harjoituksia, mukaan lukien sidosryhmät. • Harjoittelumateriaaleja hyödynnetään laajalti eri toimialoilla. • Kehitetään harjoitteluympäristöjä vastaamaan kyberuhkamaisemaa muun muassa hyödyntämällä EU-rahoitusta. • Luodaan harjoittelumahdollisuuksia myös strategiselle tasolle. • Osallistutaan monikansallisiin (Nato ja EU) kyberharjoituksiin ja kyetään toteuttamaan monikansallisia kyberharjoituksia Suomessa.	2026-2030 Lisä-resurssit	Monipuolinen sekä julkiselle hallinnolle että yksityiselle sektorille suunnattu harjoitustoiminta edistää vahvasti yhteiskunnan kyberresilienssiä ja osaamista. Kansalliset valmius- ja kyberharjoitukset tukevat myös kyberpuolustuksen valmiutta ja kehittämistä. Siviili- ja sotilastoimijat harjoittelevat säännöllisesti yhdessä. Kyberharjoitukset mahdollistavat eri toiminnan tasojen ja viranomaisten välisen toiminnan kehittämisen. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM, KTJ, HVK, VNK, PLM,** muut ministeriöt, Traficom, PV, DVV, elinkeino-elämä, järjestöt, erityisesti MPK

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
2.9.	**Varmistetaan yhteiskunnan tarvitsemien viestintäyhteyksien ja datan saatavuuden toimivuus, korjauskyky ja tarvittaessa vaihtoehtoiset yhteystavat vakavissa poikkeamatilanteissa** **Kori 1**	• Varmennetaan kansainväliset tietoliikenneyhteydet huoltovarmuuden näkökulmasta.	2025-2027 Kehittä-minen tapahtuu osana HVK:n DT2030-ohjelmaa.	Kansainvälisten tietoliikenneyhteyksien toiminta kaikissa tilanteissa on edellytys huoltovarmuuden turvaamiselle. Vaikuttavuus: kansallinen / erittäin suuri.	**HVK, LVM,** Traficom, elinkeino-elämä

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
2.10.	**Tunnistetaan yhteiskunnan eri toimialojen kyberturvallisuuden erityistarpeet ja kehitetään ratkaisuja poikkeamiin varautumiseksi ja niistä palautumiseksi** **Kori 1**	• Yhteiskunnan eri toimialojen ja kunta-alan toimijoiden jatkuvuus-, valmius- ja varautumismenettelyt ovat ajantasaisia ja käytössä. • Toimialojen ja kunta-alan toimijoilla on käytettävissään kyber- ja digitaalisen turvallisuuden koulutusaineistoja, jotka tukevat kybervarautumisessa tarvittavaa ylimmän johdon ja henkilöstön osaamista.	2025-2027 Kehittäminen tapahtuu osana HVK:n DT2030-ohjelmaa.	Kaikki toimialat ovat riippuvaisia digitaalisesta infrastruktuurista ja sen päällä toimivista palveluista. Toiminnalla pyritään parantamaan toimialakohtaista kyberturvallisuutta huoltovarmuuskriittisillä aloilla. Vaikuttavuus: kansallinen / erittäin suuri.	**HVK,** Traficom, elinkeinoelämä
2.11.	**Ylläpidetään ja tuetaan digitaalisen infran tuottajien kykyä varautua kyberhäiriöihin** **Kori 2**	• Tuetaan teleyritysten ja digitaalisen infrastruktuurin tuottajien mahdollisuuksia varautua kyberuhkiin muuttuneessa toimintaympäristössä. • Edistetään viranomaisten ja teletoimijoiden yhteistyötä matkaviestinverkkojen kehitykseen liittyvissä kysymyksissä.	2024 alkaen Toiminta-menot	Oikea-aikaisella ja luottamuksellisella yhteistyöllä voidaan parantaa digitaalisen infrastruktuurin toimijoita varautumaan kyberuhkiin ja teknologiseen murrokseen. Yhteistyöllä voidaan ennakollisesti tunnistaa uusien viestintäteknologioiden turvallisuusuhkia ja ennaltaehkäistä niitä sekä vaikuttaa kansainvälisellä yhteistyöllä viestintäinfran turvallisuuden vahvistamiseen. Vaikuttavuus: kansallinen/suuri.	**LVM,** Traficom, HVK

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
2.12.	**Parannetaan avaruuspalvelujen avulla maanpäällisten järjestelmien resilienssiä** **Kori 2**	• Tunnistetaan yhteiskunnan kriittisen infrastruktuurin riippuvuus avaruuspalveluista. • Turvataan radiotaajuuksien käytettävyys suomalaisen maa-asema- ja satelliittiliiketoiminnalle. • Parannetaan maanpäällisten järjestelmien resilienssiä hyödyntämällä avaruuspalveluita varajärjestelminä tietoliikenteessä ja aikasynkronoinnissa. • Varmistetaan avaruuspalveluiden kansainväliset toimitusketjut ja vahvistetaan kansallisten toimijoiden kotimaista omistajuutta. • Otetaan soveltuvissa kohteissa käyttöön EU:n avaruusohjelman viranomaisille ja kriittiselle infrastruktuurille tarjoamia varmennettuja satelliittipalveluita. • Seurataan kyberturvallisuutta osana avaruustilannekuvaa yhteistyössä eri toimijoiden kanssa. • Huomioidaan avaruusjärjestelmien kyberturvallisuus luvissa, lupaehdoissa ja järjestelmien elinkaaren hallinnassa.	2025-2030 Toiminta-menot	Avaruuspalveluiden saatavuus ja palveluiden jatkuvuus paranevat. Kriittinen infrastruktuuri pystyy tukeutumaan avaruuspalveluihin ja toisaalta varautumaan niiden häiriöihin. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**LVM, TEM, SM,** VNK, HVK, Traficom

Pilari II: Varautuminen ”Vahva yhteiskunnan kyberresilienssi ja toimintavarmuus”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
2.13.	**Parannetaan laitteiden ja ohjelmistojen tietoturvaa varmistamalla EU:n kyberkestävyys-säädöksen (CRA) sujuva ja tehokas toimeenpano** **Kori 1**	• Edistetään digitaalisen elementin sisältävien laitteiden ja ohjelmistojen valmistajien markkinoille pääsyä ja kilpailua EU:n sisämarkkinoilla. • Varmistetaan viranomaisen kyky hyväksyä sujuvasti riittävä määrä kolmannen osapuolen arviointia tekeviä ilmoitettuja laitoksia ja siten ehkäistä markkinoille tulon pullonkauloja. • Edistetään laitteiden ja ohjelmistojen tietoturvan tasoa ohjeistamalla yrityksiä uusista vaatimuksista sekä järjestämällä niiden markkinavalvonta asianmukaisesti ja sujuvasti. • Varmistetaan Kyberturvallisuuskeskuksen kyky koordinoida ilmoituksia laitteiden ja ohjelmistojen haavoittuvuuksista asetuksen edellyttämällä tavalla. • Tuetaan kyberturvallisuussertifioinnin toimivaltaisen viranomaisen tehtäviä sertifiointien kysynnän kasvaessa kyberkestävyyssäädöksen toimeenpanon johdosta.	2026-2030 Toiminta-menot, osin lisä-resurssit	Kyberkestävyyssäädös on keskeinen uusi EU-asetus, jolla asetetaan tietoturvaa koskevat vähimmäisvaatimukset internetiin tai toiseen laitteeseen kytkettävissä oleville laitteille ja ohjelmistoille. Asetuksen soveltaminen alkaa vaiheittain vuosien 2026–2027 aikana. Asetuksen onnistuneella toimeenpanolla on huomattava merkitys laitteiden ja ohjelmistojen käytön tietoturvalle sekä suomalaisten yritysten kilpailukyvylle eli laite- ja ohjelmistovalmistajien EU-markkinoille pääsyyn ja kilpailuun sisämarkkinoilla. Asetuksella varmistetaan, että tuotteissa on vähemmän haavoittuvuuksia ja että valmistajat vastaavat kyberturvallisuudesta tuotteen koko elinkaaren ajan. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri	**LVM,** Traficom

Pilari III: Yhteistoiminta ”Vankka kansallinen ja kansainvälinen yhteistoimintamalli”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
3.1.	**Kehitetään kansallista kyberpolitiikkaa koskevien tavoitteiden yhteensovittamista Suomen kansainvälisen profiloitumisen ja vaikuttavuuden edistämiseksi** **Kori 1**	• Kehitetään Suomen aktiivista osallistumista keskeisiin kahden- ja monenvälisiin verkostoihin ja yhteistoimintaan sekä vaikutetaan aktiivisesti kansainvälisissä järjestöissä, etenkin EU:ssa ja Natossa. • Luodaan kansallinen koordinaatiomalli kansainvälisestä kyberturvallisuuden ja -puolustuksen yhteistoiminnasta. • Toteutetaan aktiivista strategista ja operatiivista yhteistoimintaa avainmaiden kanssa. • Vaikutetaan kyberturvallisuusnäkökohtien huomioimiseen EU-sääntelyssä ja kansainvälisissä sopimuksissa. • Pyritään edistämään Suomen kokonaisturvallisuuteen ja varautumiseen pohjautuvan yhteistoimintamallin soveltamista kansainvälisesti.	2024 alkaen Toiminta-menot	Suomi on saavuttanut asettamansa kriittiset tavoitteet kansainvälisessä kontekstissa. Tarvittavat järjestelyt ja sopimukset on tehty sekä strateginen ja operatiivinen yhteistyö käynnistynyt. EU-Nato yhteistyö tukee Suomen kyberturvallisuutta ja –puolustusta. Kansainvälistä kyberpolitiikkaa koskeva kansallinen tilannekuva- ja yhteensovittamismalli on luotu ja vakiinnutettu. Suomi on aktiivisesti myötävaikuttanut EU-Nato -yhteistyön painopistealueiden ja päätoimintojen kehittymiseen kansallista kyberturvallisuutta ja -puolustusta tukevaan suuntaan. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**UM, VNK, KTJ, PLM,** LVM, Traficom, PV
3.2.	**Kehitetään kansainvälisen terveystietojen vaihdon turvallisuutta** **Kori 1**	• European Health Data Space / sosiaali- ja terveystietojen ensio- ja toisiokäytön toimeenpanon valmistelu- ja toimeenpanovaiheessa tehdään riskiarvio.	2025-2031 Toiminta-menot	Varmistetaan kansallisesti kyberturvataso vastaamaan EU:n tiedonvaihdon toimintaympäristöä. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**STM,** KELA, THL, Valvira

Pilari III: Yhteistoiminta ”Vankka kansallinen ja kansainvälinen yhteistoimintamalli”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
3.3.	**Toteutetaan viranomaisten toimintaedellytykset kyberturvallisuudessa -selvityksen toimenpiteet niiltä osin, kun eivät ole osana muita toimenpiteitä** **Kori 1**	• Parannetaan viranomaisten keskinäistä ja yksityisen sektorin yhteistoimintaa ja prosesseja sekä tiedonvaihtoa varautumisessa ja vasteessa, mukaan lukien lainsäädäntö. • Tunnistetaan yhteiskunnan elintärkeitä toimintoja tuottavat tahot toimitusketjuineen. • Päivitetään kyberturvallisuuden sanasto. • Huomioidaan kybertoimintaympäristö valmiuslainsäädännössä ja toteutetaan lainsäädäntömuutokset, joilla mahdollistetaan kriittisten yritysten avustaminen. • Kehitetään yhteiset korkeasti turvallisuusluokitellun tiedon tekniset tiedonvaihtoratkaisut.	2025-2030 Osin lisä-resurssit	Mahdollistetaan tehokas yhteistoiminta julkisessa hallinnossa turvallisuusluokitellun ja erityissuojattavan tiedon käsittelyn edistyneillä ratkaisuilla. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**SM, PLM, UM, VM, LVM,** KTJ, VNK, OM, Traficom, PV, Valtori, KRP, Supo

Pilari III: Yhteistoiminta ”Vankka kansallinen ja kansainvälinen yhteistoimintamalli”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
3.4.	**Selkiytetään vastuita kansallisen kyberpuolustuksen kehittämisessä** **Kori 1**	• Kuvataan kyberpuolustusdoktriinissa kansallisen kyberpuolustuksen yhteistoiminnan toimintamalli. • Viranomaisten operatiivinen yhteistoimintarakenne mahdollistaa viranomaisten operatiivisen yhteistoiminnan koordinoinnin myös kyberpuolustuksen tehtävissä kaikissa oloissa. • Kehitetään yhteistoimintaa, tiedonvaihtoa ja vastetta huomioiden eri sektorien väliset tarpeet, mukaan lukien lainsäädäntö: siviili-sotilasyhteistyö, viranomaisten ja yksityisen sektorin yhteistyö, puolustus- ja turvallisuussektorin yhteistyö, vapaaehtoisen maanpuolustuksen yhteistyö.	2025-2032 Lisä-resurssit	Eri tasojen yhteistoimintarakenteet on muodostettu, toiminta on käynnissä ja sillä on kehittämissuunnitelma. Yhteistoimintaa on kehitetty tukemaan kyberpuolustuksen tilanneymmärryksen muodostumista ja tehtävien (mukaan lukien vastatoimet) toimeenpanoa. Kyberpuolustus kykenee tukemaan koordinoidusti tiedoillaan ja suorituskyvyillään muita viranomaisia ja sektoreita. Suomi näyttäytyy kyberpuolustuksessa yhtenäisenä toimijana. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**PLM, PV,** muut minis-teriöt ja viran-omaiset, HVK, elinkeino elämä, järjestöt

Pilari III: Yhteistoiminta ”Vankka kansallinen ja kansainvälinen yhteistoimintamalli”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
3.5.	**Varmistetaan ajantasaisen kyberturvallisuuden ohjeistuksen helppo saatavuus julkisen hallinnon, yritysten, kansalaisten ja järjestöjen käyttöön** **Kori 2**	• Luodaan ja ylläpidetään kansallista kyberturvaohjeistuksen tietopankkia ja palvelukatalogia mukaan lukien sote-ohjeet. • Kootaan julkisen hallinnon hyvät käytänteet kyberturvallisuuden toteuttamiseksi ja jaetaan ne yhteisesti hyödynnettäviksi yhteisen kanavan kautta.	2024-2028 Toiminta-menot	Yhteinen ohjeistustietopankki tehostaa kyberturvallisuuden parantamistoimia ja yhteistoimintaa yhteiskunnassa. Vaikuttavuus: kansallinen/suuri.	**VM, STM**, DVV

Pilari III: Yhteistoiminta ”Vankka kansallinen ja kansainvälinen yhteistoimintamalli”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
3.6.	**Kehitetään kyberturvallisuuden tilannekuvan tuotantoa ja jakelua sekä vahvistetaan eri organisaatioiden tilannetietoisuutta** **Kori 1**	• Kehitetään strategista tilannekuvan tuotantoa palvelemaan kohderyhmien tarpeita ja huolehditaan, että kyberturvallisuustapahtumat välittyvät Valtioneuvoston tilannekeskukselle. • Varmistetaan Traficomin Kyberturvallisuuskeskuksen tilannekuvatuotteiden jatkuvuus ja saatavuus oikeille kohderyhmille. • Kehitetään yhteistyöverkostojen toimintaa vastaamaan muuttunutta toimintaympäristöä ja turvataan verkostojen toiminta. • Kehitetään valvovien viranomaisten (NIS2) ja tietosuojavaltuutetun yhteistyötä ja yhteistä poikkeamanhallintaa.	2025-2027 Lisä-resurssit	Tilannekuvan kohderyhmien tarkastelulla varmistetaan oikea-aikaisen tilannekuvatiedon saatavuus laajalti yhteiskunnassa. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM**, **VNK,** Traficom, TSV, muu julkinen hallinto

Pilari III: Yhteistoiminta ”Vankka kansallinen ja kansainvälinen yhteistoimintamalli”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
3.7.	**Julkinen sektori yhdessä yksityisen sektorin kanssa kehittää ja tarjoaa keskitettyjä kyberturvallisuus-palveluja** **Kori 1**	• Varmistetaan Traficomin Kyberturvallisuuskeskuksen tuottamien palveluiden jatkuvuus ja laajennetaan palveluiden, kuten Kybermittarin ja Hyökyn käyttöä laajemmille kohderyhmille. • Vahvistetaan DVV:n Vahti-verkoston, Taisto-harjoitusten ja Julkri-työkalun vaikuttavuutta. • Kasvatetaan DVV:n hallinnollisen digiturvan kokonaiskuvapalvelun käyttöastetta, vaikuttavuutta ja hyödyntämistä julkisessa hallinnossa. • Tuotetaan mallipohjia, neuvotellaan keskitetysti sopimuksia. • Tunnistetaan ja kehitetään tarvittavia uusia palveluita.	2024-2030 Toiminta-menot, osin lisäresurssit	Yhteiset keskitetyt kyberturvallisuuspalvelut tehostavat resurssien käyttöä. Niiden laaja käyttö on edellytys merkittävälle julkisten palveluiden turvallisuuden ja toimintavarmuuden parantamiselle. Palveluiden jatkuvuuden turvaaminen, uudet palvelut ja palveluiden laajennukset edellyttävät lisäresursseja. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM**, **VM,** HVK, Traficom, DVV, julkisen hallinnon ICT-yhtiöt, yksityinen sektori, muu julkinen hallinto

Pilari III: Yhteistoiminta ”Vankka kansallinen ja kansainvälinen yhteistoimintamalli”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
3.8.	**Edistetään yhteisten tieto- ja viestintäteknisten palveluiden ja tietovarantojen turvallisuutta ja toimintavarmuutta** **Kori 1**	• Toteutetaan yhteisten tieto- ja viestintäteknisten palveluiden turvallisuuden kehittämisohjelma (Pato). • Turvataan kriittiset tietovarannot ja kriittisten kohteiden paikkatiedot. • Varmistetaan operatiivinen tiedonvaihto ja johtaminen yhteisellä turvallisella tiedonvaihtoratkaisulla kriittisen viestinnän takaamiseksi.	2024-2030 Toiminta-menot	Yhteiset toimintavarmat tieto- ja viestintätekniset palvelut tukevat yhteiskunnan häiriötöntä toimintaa ja mahdollistavat strategisten tehtävien tehokkaan toteuttamisen. Vaikuttavuus: kansallinen / erittäin suuri.	**VM,** Valtori, ERVE
3.9.	**Uudistetaan turvallisuusverkkoa ja yhteisiä tieto- ja viestintäteknisiä palveluita koskevat säännökset** **Kori 2**	• Mahdollistetaan viranomaisten kyberkyvykkyyksien hyödyntäminen valtiohallinnon yhteisten tieto- ja viestintäteknisten palvelujen tuotannon suojaamisessa säännöksin ja sopimuksin.	2026-2029 Toiminta-menot	Viranomaisten resursseja käytetään mahdollisimman tehokkaasti yhteisten tieto- ja viestintäteknisten palvelujen tuotannon ja yhteiskunnan turvallisuusstrategian (YTS) mukaisten strategisten tehtävien turvaamisessa. Vaikuttavuus: kansallinen/suuri.	**VM,** PLM, PV, Valtori

Pilari III: Yhteistoiminta ”Vankka kansallinen ja kansainvälinen yhteistoimintamalli”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
3.10.	**Selvitetään turvallisuusluokittelua koskevien säännösten kehitystarpeita** **Kori 1**	• Selvitetään turvallisuusluokittelusäännösten soveltuvuus pilvipalvelut ja tekoäly huomioiden sekä toteutetaan tarvittavat säädösmuutokset. • Selvitetään turvallisuusluokittelu-velvoitteen soveltamisala ja selkiytetään ohjeistusta erityisesti hyvinvointialueilla, kunnissa ja erityistehtäväyhtiöissä sekä toteutetaan tarvittaessa säädösmuutokset. • Mahdollisten säädösmuutosten yhteydessä tarkastetaan yhteensopivuus kansainvälisten säädösten kanssa.	2025-2029 Toiminta-menot	Turvallisuusluokittelusäännösten ajantasaisuus ja luokitteluvelvoitteen tarkoituksenmukainen soveltamisala ja ohjeistus parantavat kansallista kyberturvallisuutta. Vaikuttavuus: kansallinen/suuri.	**VM, UM**

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
4.1.	**Kehitetään hyvinvointialueiden valmiuksia ja kykyä varautua ja reagoida oikea-aikaisesti kyberhäiriöihin** **Kori 2**	• Hyvinvointialueet ovat luokitelleet keskeiset tietojärjestelmänsä ja toimintonsa yhtenäisen kriittisyysluokittelun mukaisesti. • Selkeytetään poikkeamien ilmoittamismenettelyt hyvinvointialueilla. • Vahvistetaan sosiaali- ja terveydenhuollon valmiuskeskusten (5) ja kansallisten toimijoiden yhteistyöverkostoa ja otetaan käyttöön uusi hyvinvointialueiden riskienhallintamalli ICT-häiriöhallinnan kehittämiseksi. • Varmistetaan sosiaali- ja terveyshuollon kansallisten palveluiden turvallisuus.	2024-2030 Toiminta-menot, osin lisäresurssit Kehittä-minen tapahtuu myös osana HVK:n DT2030-ohjelmaa	Hyvinvointialueiden kyky varautua ja reagoida toimintaympäristön kyberuhkiin paranee. Ylläpidetään tietoisuutta kyberturvallisuudesta osana sote-organisaatioiden toiminnan kehittämistä. Vaikuttavuus: kansallinen/suuri.	**STM, OM**, VM, SM, hyvin-vointi-alueet, Traficom, Valvira, TSV, elinkeino-elämä

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
4.2.	**Kehitetään kuntien valmiuksia ja kykyä varautua ja reagoida oikea-aikaisesti kyberhäiriöihin** **Kori 2**	• Vahvistetaan riskienhallintaa, jatkuvaa parantamista, turvallisuuskulttuuria ja parhaiden käytäntöjen jakamista mukaan lukien VIRT-toiminta (Virtual Incident Response Team), ICT-varautuminen, häiriönhallinta, turvalliset hankinnat ja pilvipalveluiden turvallisuus soveltuvissa kansallisissa, alueellisissa ja paikallisissa kuntien välisissä verkostoissa. • Ylläpidetään ja kehitetään olennaisia kansallisia tietoturva- ja tietosuojaverkostoja organisaatioiden välisen vertaisverkostoitumisen ja vertaistiedon jakamisen mahdollistamiseksi. • Kunnat toteuttavat keskeisten tietojärjestelmien ja toimintojen kriittisyysluokittelun.	2024-2030 Toiminta-menot Kehittä-minen tapahtuu myös osana HVK:n DT2030-ohjelmaa	Kuntien kyky varautua ja reagoida toimintaympäristön kyberuhkiin paranee. Vaikuttavuus: kansallinen/merkittävä.	**VM**, kunnat, DVV, Traficom, muu julkinen hallinto, elinkeino-elämä

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
4.3.	**Vahvistetaan kriittisten toimialojen varautumista ja reagointia kyberpoikkeama-tilanteisiin** **Kori 2**	• Tuetaan kriittisten toimialojen varautumista ja vastaamista kyberhäiriöihin ja henkilötietojen tietosuojaloukkaustilanteisiin muun muassa EU:n kyberturvallisuuden hätätilanteiden mekanismia hyödyntämällä. • Edistetään suomalaisten tietoturvapalveluntarjoajien osallistumista EU:n kyberturvallisuusreserviin. • Hyödynnetään EU:n kyberturvallisuusreservin palveluita merkittäviin tai laaja-alaisiin poikkeamatilanteisiin vastaamisessa. • Parannetaan tietosuojavaltuutetun toimintaedellytyksiä.	2025 alkaen Osin lisäresurssit	Mahdollistaa tai nopeuttaa kyberturvallisuutta parantavien toimenpiteiden toteuttamisen organisaatioissa ja sitä kautta parantaa organisaatioiden valmiuksia ja kykyä varautua ja reagoida oikea-aikaisesti kyberturvallisuushäiriöihin. EU-rahoitteisissa varautumistoimenpiteissä vaatimus 50 % kansalliseen vastinrahoitukseen. Vaikuttavuus: kansallinen/suuri.	**LVM, OM,** Traficom, TSV

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
4.4.	**Turvataan kansallinen havainnointikyky (HAVARO)** **Kori 1**	• Turvataan HAVARO-palvelun toiminta ja jatkuvuus. (HAVARO = kansallinen vakavien tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä). • Edistetään HAVAROn hyödyntämistä yhteiskunnan elintärkeiden toimintojen turvaamisessa.	2026-2030 Lisä-resurssit	HAVARO-palvelu tuottaa tietoa, jonka avulla palvelua käyttävät organisaatiot rakentavat ja kehittävät omaa kybersuojaustaan. HAVAROn jatkuvuuden turvaamisella varmistetaan kansallinen havainnointikyky ja ylläpidetään kansallista kyberturvallisuutta. Vaikuttavuus: kansallinen / erittäin suuri.	**LVM,** Traficom, HVK

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
4.5.	**Varmistetaan tiedusteluviranomaisten riittävä tiedonhankintakyky** **Kori 2**	• Kehitetään kykyä valtiollisen kybervakoilun ja vaikuttamisen havainnoimiseksi ja varmistetaan sen resurssit. • Kehitetään kybertiedustelua vastaamaan toimintaympäristön muutosta.	2025-2035 Lisä-resurssit	Kybervakoilun havainnoinnilla on keskeinen merkitys uhkan tunnistamiselle ja vaikutusten rajaamiselle. Vaikuttavuus: kansallinen ja kansainvälinen / suuri.	**SM**, **PLM,** PV, Supo

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa / toimijat
4.6.	**Kehitetään viranomaisten yhteistyötä, tilannekuvaa ja uhkien havainnointia ja vahvistetaan osallistumista kansainväliseen yhteistyöhön** **Kori 2**	• Vahvistetaan kansallista viranomaisyhteistyötä, tilannekuvaa ja havainnointikykyä hyödyntämällä EU:n kyberturvallisuuden hälytysjärjestelmän rahoitusmahdollisuuksia. • Vahvistetaan kansainvälistä yhteistyötä osallistumalla kybersolidaarisuussäädöksen mukaiseen rajat-ylittävään tilannekuvayhteistyöhön. • Luodaan Traficomin Kyberturvallisuuskeskukseen kansallinen kyberturvallisuuden keskittymä rajat-ylittävään yhteistyöhön osallistumiseksi ja kansallisen tilannekuvan ja uhkatiedon jakamisen tehostamiseksi.	2025-2032 Osin lisäresurssit	Tehokkaalla uhkien havainnoinnilla ja tilannekuvan jakamisella voidaan ennaltaehkäistä kyberhäiriötilanteita ja pienentää niiden vaikutuksia. Osallistumalla EU-tason tilannekuva- ja havainnointikyvyn yhteishankintoihin voidaan saavuttaa säästöjä, tehostaa tilannekuvan keräämistä ja nopeuttaa uhkien havainnointia EU-jäsenmaiden kanssa. Vaikuttavuus: kansallinen ja kansainvälinen / suuri.	**LVM, VNK PLM, SM,** Traficom, PV, muut turvalli-suus-viran-omaiset

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
4.7.	**Turvataan vakavan ja järjestäytyneen tietoverkko- sekä tietoverkkoavusteisen rikosten torjunnan sekä kyberpuolustuksen resurssit** **Kori 1**	• Rikostorjunnan ja -tutkinnan kyvykkyyden varmistaminen ja kehittäminen sekä rikosvastuun toteuttaminen. • Kehitetään rikostorjunnan ja kyberpuolustuksen yhteistyötä erityisesti valtiolliseen toimintaan liittyvissä tapauksissa.	2024 alkaen Toiminta-menot	Rikosvastuun toteuttamisen sekä yhteiskunnan häiriöttömän toiminnan kannalta on tärkeää, että poliisilla on riittävä kyky tutkia vakavan ja järjestäytyneen tietoverkkorikollisuuden tapaukset sekä tarjota tukea muiden maiden lainvalvontaviranomaisten toiminnalle. Vastaava kyvykkyys on tarpeen Puolustusvoimien tehtävien toteuttamiseksi kyberpuolustuksessa ja lain sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa määrittelemässä laajuudessa. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri	**SM**, PLM, Poliisi-hallitus
4.8.	**Vakiinnutetaan kansainvälinen rikostorjuntayhteistyö tietoverkkorikosten torjunnassa (J-CAT)** **Kori 2**	• Vakiinnutetaan kyberrikostorjunnan kansainvälinen operatiivinen toiminta. Varmistetaan kansainvälisen vakavan ja järjestäytyneen rikollisuuden torjunnan mahdollistava operatiivinen yhteistyö.	2024 alkaen Toiminta-menot	Vakava kyberrikollisuus on määritelmällisesti kansainvälistä ja J-CAT yhteistyö on osoittanut kansainvälisen operatiivisen työn välttämättömyyden, jolle J-CAT tarjoaa toimivan alustan. Vaikuttavuus: kansallinen ja kansainvälinen / suuri.	**SM**, Poliisi-hallitus, KRP

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Konkreettiset tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
4.9.	**Tiivistetään viranomaisten välistä yhteistyötä tietoverkkoavusteisen rikollisuuden tilannekuvan parantamiseksi ja ennaltaehkäisemiseksi** **Kori 2**	• Selvitetään tyypillisimmät rikosten tekotavat, niiden yleisyys ja niiden ehkäisyyn hyvät käytännöt sekä selvitetään näiden aiheuttamat rikosvahingot. • Tilannekuvan perusteella vaikutetaan tunnistettuihin uhkiin ja toimijoihin. • Valistetaan kansalaisia hyvien käytäntöjen avulla. • Kehitetään verkkokauppahuijausten torjunnan moniviranomaisyhteistyötä ja yhteistyötä verkkokauppatoimijoiden (elinkeinoelämä) kanssa.	2025 alkaen Toiminta-menot	Parannetaan tietoverkkoavusteisen rikollisuuden tilannekuvaa ja sen perusteella vaikutetaan tyypillisimpien tekotapojen ennaltaehkäisyyn. Vaikuttavuus: kansallinen/suuri.	**OM, SM, TEM,** Rikoksen torjunta-neuvosto Poliisi, Traficom KKV, kuluttaja-asiamies, TSV

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
4.10.	**Valmistellaan kansallinen attribuutiokehikko** **Kori 1**	• Luodaan kansallinen attribuutiokehikko. • Selkeytetään prosessit, viranomaisroolit ja -vastuut (tekninen, operatiivinen ja poliittinen).	2024 alkaen Toiminta-menot	Attribuutiokehikko tukee Suomen ulko- ja turvallisuuspolitiikan vaikuttavuutta mm. kehittämällä reagointivalmiutta vihamieliseen kybertoimintaan sekä edistämällä sääntöpohjaisuutta ja vastuullista valtiokäyttäytymistä kybertoimintaympäristössä. Attribuutiokehikko kehittää kykyä ja valmiutta attribuoida Suomeen kohdistuvia kyberuhkatapauksia sekä osoittaa tukea kansainvälisille järjestöille ja kumppaneille. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**UM,** VNK**,** SM, PLM, LVM, KTJ, TPK, tiedustelu viran-omaiset, Traficom, PV, KRP

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
4.11.	**Laaditaan kyberpuolustusdoktriini** **Kori 1**	• Laaditaan ja hyväksytään doktriini. • Tunnistetaan ja selkeytetään prosessit, viranomaisroolit ja -vastuut kyberpuolustuksessa. • Kuvataan valtiollisen suvereniteetin valvonnan, suojaamisen ja turvaamisen periaatteet. • Päivitetään Suomen periaatepäätös kansainvälisen lainsäädännön soveltamisesta. • Kehitetään kybervastatoimien ja -operaatioiden vaikuttavuuden arvioinnin perusteet niin strategiselle kuin operatiiviselle tasolle.	2024-2026 Toiminta-menot	Kyberpuolustusdoktriinilla luodaan kyky kokonaisvaltaiseen ja koordinoituun vasteeseen ja vastatoimiin vihamieliseen toimintaan. Kehitetään yhteistyötä ja päämäärätietoisuutta. Kehitetään kykyä tukea liittolaisia ja hyödyntää liittolaisten kykyjä kansallisessa kyberpuolustuksessa. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**PLM**, **UM,** VNK, SM, LVM, TPK, PV, KTJ, Traficom, Supo, Poliisi

Pilari IV: Reagointi ja vastatoimet ”Oikea-aikainen uhkiin reagointi ja turvattu suvereniteetti”

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa/ toimijat
4.12.	**Kehitetään kansallista ja sotilaallista kyberpuolustusta ja saatetaan loppuun niiden integraatio Natoon** **Kori 1**	• Päivitetään kyberpuolustuksen tehtävien ja toimivallan säädöspohja. • Päivitetään valtiollisen suvereniteetin turvaamisen säädöspohja. • Jatketaan kyberpuolustuksen suorituskyvyn kehittämistä kansallisella, operatiivisella ja paikallisella tasolla. • Mahdollistetaan joustava virka-apu ja sen kaltainen apu eri viranomaisten välillä. • Kokonaismaanpuolustuksen ja puolustusjärjestelmän integraatio valmis kyberturvallisuuden osalta. • Kansallinen resilienssityö toteutettu ja viety varautumissuunnitelmiin ja harjoiteltu.	2024-2032 Osin lisäresurssit	Turvataan valtiollinen suvereniteetti. Luodaan kyky kansalliseen kokonaisvaltaiseen ja koordinoituun vasteeseen ja vastatoimiin. Suomi kykenee toimimaan osana liittokuntaa ja sen pelotetta ja puolustusta myös kybertoimintaympäristössä. Suomi kykenee antamaan ja vastaanottamaan apua. Suomi kykenee tukemaan alueella toimivia liittolaisjoukkoja myös kiistetyssä kyberympäristössä. Vaikuttavuus: kansallinen ja kansainvälinen / erittäin suuri.	**PLM, PV,** UM, LVM, SM, muut minis-teriöt, muut viran-omaiset ja paikallis- ja aluetason toimijat, kriittinen yritys-kenttä

Strategian toteuttamiseen liittyvät muut toimet

Nro	Toimenpide	Tavoitteet	Aikataulu ja rahoitus	Vaikutusarvio ja vaikuttavuusanalyysi	Vastaa, toimijat
	Suomi tuottaa tiedot kansainvälisten kyberturvallisuus-indeksien kyselyihin (Kansainvälisen televiestintäliiton ITUn kyberturvallisuusindeksi (Global Cyber Index, GCI) ja kansallinen kyberturvallisuusindeksi (e-Governance Academyn National Cyber Security Index, NCSI)	• Suomi sijoittuu kärkimaiden joukkoon kansainvälisten indeksien mittauksissa.	2026 alkaen Toiminta-menot	Mittareita hyödynnetään kansallisen kehitystyön tukena. Vaikuttavuus: kansallinen / erittäin suuri.	**KTJ**, strate-gian seuranta-ryhmä

“Suojattu Suomi – Yhteistyössä kohti kyberturvallista tulevaisuutta.”

VALTIONEUVOSTO
STATSRÅDET