Utvecklingsprogram för cybersäkerheten

KOMMUNIKATIONS-
MINISTERIET

Kommunikations-
ministeriets
publikationer **2021:8**

lvm.fi/sv

Kommunikationsministeriets publikationer 2021:8

Utvecklingsprogram för cybersäkerheten

Rauli Paananen

Kommunikationsministeriet Helsingfors 2021

Julkaisujen jakelu
Distribution av publikationer

Valtioneuvoston julkaisuarkisto Valto

Publikations-
arkivet Valto

julkaisut.valtioneuvosto.fi

Julkaisumyynti
Beställningar av publikationer

Valtioneuvoston verkkokirjakauppa

Statsrådets
nätbokhandel

vnjulkaisumyynti.fi

Kommunikationsministeriet

ISBN pdf: 978-952-243-603-0
ISSN pdf: 1795-4045

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2021

Presentationsblad
10.6.2021

Utvecklingsprogram för cybersäkerheten

Kommunikationsministeriets publikationer 2021:8
Utgivare Kommunikationsministeriet

Författare Rauli Paananen
Språk svenska
Sidantal 45

Referat

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

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

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

Nyckelord datasäkerhet, cybersäkerhet, digitalisering, riskhantering

ISBN PDF 978-952-243-603-0
ISSN PDF 1795-4045
Ärendenummer VN/797/2021

URN-adress http://urn.fi/URN:ISBN:978-952-243-603-0

Kuvailulehti
10.6.2021

Kyberturvallisuuden kehittämisohjelma

Liikenne- ja viestintäministeriön julkaisuja 2021:8
Julkaisija Liikenne- ja viestintäministeriö

Tekijä/t Rauli Paananen
Kieli ruotsi **Sivumäärä** 45

Tiivistelmä

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

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

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

Asiasanat tietoturva, kyberturvallisuus, riskienhallinta, digitalisaatio

ISBN PDF 978-952-243-603-0 **ISSN PDF** 1795-4045
Asianumero VN/797/2021

Julkaisun osoite http://urn.fi/URN:ISBN:978-952-243-603-0

Description sheet
10 June 2021

Cyber Security Development Programme

Publications of the Ministry of Transport and Communications 2021:8
Publisher Ministry of Transport and Communications

Authors Rauli Paananen
Language Swedish **Pages** 45

Abstract

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

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

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

Keywords information security, cyber security, risk management, digitalisation

ISBN PDF 978-952-243-603-0 **ISSN PDF** 1795-4045
Reference number VN/797/2021

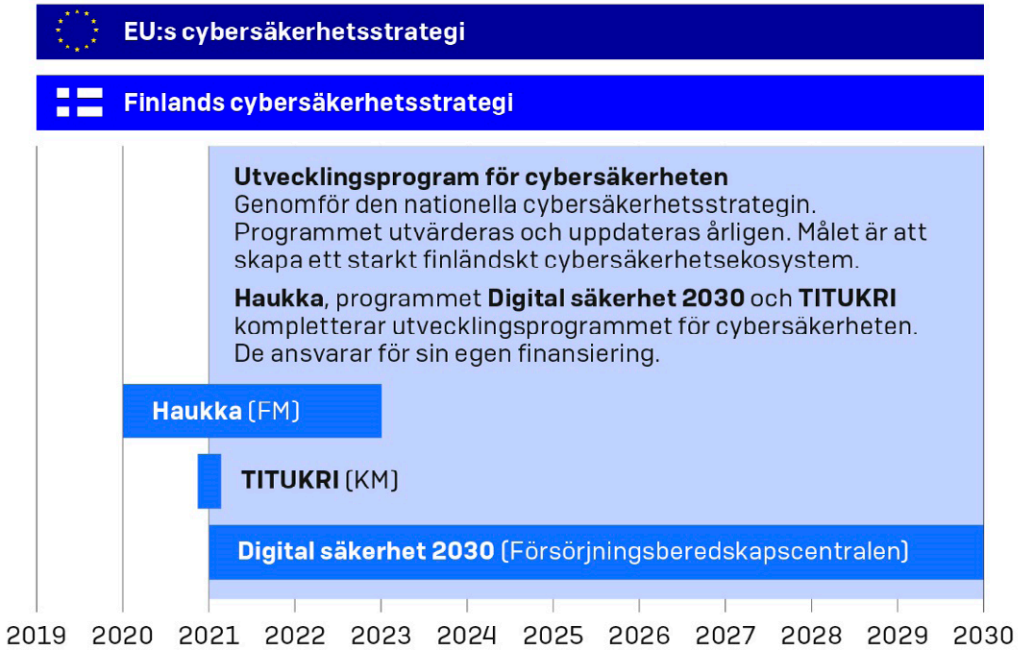
URN address http://urn.fi/URN:ISBN:978-952-243-603-0

Innehåll

1 Inledning

I statsminister Sanna Marins regeringsprogram har man satt som mål att utveckla den nationella cybersäkerheten med avseende på förbättring av lägesbilden, fördjupat internationellt samarbete och effektivisering av den nationella samordningen. I statsrådets principbeslut om Finlands cybersäkerhetsstrategi, som gavs 2019, identifieras ett behov av att förbättra helhetsläget i fråga om den nationella cybersäkerheten. Cybersäkerhetsstrategin är en del av verkställandet av säkerhetsstrategin för samhället (2017) och EU:s cybersäkerhetsstrategi. Detta principbeslut om utveckling av den nationella cybersäkerheten svarar mot de ovannämnda målen.

Figur 1. Utvecklingsprogrammet för cybersäkerheten och dess centrala delar



Haukka: Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023. Programmet syftar till utveckling av tjänsterna för digital säkerhet inom den

TITUKRI: Rapport om ändringsbehoven i lagstiftningen och andra åtgärder för att förbättra datasäkerheten och dataskyddet inom kritiska

Digital säkerhet 2030: Programmet har i uppgift att utveckla den digitala infrastrukturen i samhället samt störningståligheten och cybersäkerheten hos

De åtgärdsförslag som läggs fram i slutrapporten från arbetsgruppen Förbättring av datasäkerheten och dataskyddet inom kritiska sektorer i samhället (TITUKRI) är viktiga för samhället och stöder de åtgärder som läggs fram i utvecklingsprogrammet för cybersäkerheten. Statsrådets principbeslut om digital säkerhet inom den offentliga förvaltningen och genomförandeplanen för detta samt Försörjningsberedskapscentralens program Digital säkerhet 2030 kompletterar detta principbeslut och ansvarar för sin egen finansiering. Som helhet handlar det om ett mycket omfattande och heltäckande åtgärdspaket som syftar till att utveckla cybersäkerheten i samhället (bild 1).

De betydande förändringarna i samhällsmiljön, cybersäkerhetshoten som är under ständig utveckling, den ökade komplexiteten i IKT-miljöerna, konvergensen mellan inbyggda och traditionella IKT-system och de utvecklingsobjekt som har observerats i den nationella verksamheten har alla bidragit till behovet av att förbättra helhetsläget i fråga om cybersäkerheten. Att cybersäkerhetshot realiseras orsakar även större konsekvenser än tidigare för de kritiska funktionerna och dataskyddet i det starkt nätverksbaserade samhället. Samhället är allt mer beroende av den digitala verksamhetsmiljön, och cybersäkerhet ska därför vara inbyggd i all verksamhet, alla processer och alla system som är förknippade med hotfaktorer. En god nivå på cybersäkerheten kan uppnås endast om varje aktör som är anknuten till det digitala samhället tar sitt ansvar för förverkligandet av cybersäkerhet. Cybersäkerhet ska ses som en naturlig del av det samhällsansvar som varje organisation och individerna bär.

Tidsspannet för utvecklingsprogrammet är 2021–2030, och programmet redogör för de lång- och kortsiktiga målen och fokusområdena för utvecklingen av cybersäkerheten. Genomförandeplanen för utvecklingsprogrammet beskriver i sin tur de åtgärder, inklusive ansvarsområden och mätare, som behövs för att nå målen. Effektiviteten av åtgärderna i utvecklingsprogrammet har bedömts ur internationellt och nationellt perspektiv samt ur förvaltnings- och sektorperspektiv, företagsperspektiv och medborgarperspektiv med beaktande av nuläget och målbilden samt i tillämpliga delar de nödvändiga investeringarna. En utvärdering av genomförandeplanens aktualitet och en uppdatering av åtgärderna görs varje år. För att genomföra utvecklingsprogrammet krävs finansiering på 5,9 miljoner euro årligen under perioden 2022–2025. Beslut om finansieringen av utvecklingsprogrammet fattas när planen för den offentliga ekonomin och statsbudgeten bereds. Den statliga finansiering som åtgärderna eventuellt kräver genomförs inom ramen för statsfinanserna, vid behov genom att ändra allokeringen av anslagen.

Genomförandet av utvecklingsprogrammet för cybersäkerhet och utvecklingsåtgärdernas aktualitet följs regelbundet upp av Kommunikationsministeriet och Säkerhetskommittén. Verkställandet av utvecklingsprogrammet inleds omedelbart.

Genomförandet av utvecklingsprogrammet stöder den samordningsmodell för cybersäkerhetsledningen som har fastställts i cybersäkerhetsstrategin. I samordningsmodellen beaktas den offentliga förvaltningens och näringslivets planering och utveckling av cybersäkerheten samt deras cybersäkerhetssamarbete. Cybersäkerhetsdirektören, som har placerats vid Kommunikationsministeriet, har i uppgift att utveckla samarbetet och kompetensen i cybersäkerhetsmiljön inom olika sektorer. Som en del av detta utvecklingsprogram förbättras dessutom skapandet av en operativ lägesbild och den operativa ledningen vid omfattande cybersäkerhetsstörningar. Dessutom beaktas den internationella verksamhetsmiljön samt processerna och praxisen på det internationella planet, som syftar till att förbättra cybersäkerheten inom bl.a. EU.

Över 80 olika organisationer deltog i beredningen av utvecklingsprogrammet. I de workshoppar som ordnades i samband med beredningen deltog bl.a. näringslivet, cybersäkerhetsindustrin, statsförvaltningen, universiteten och olika organisationer.

2 Utvecklingsprogrammets mål och huvudteman

Utvecklingsprogrammet för cybersäkerheten närmar sig den nationella cybersäkerheten framför allt med möjligheterna som utgångspunkt. Om möjligheterna realiseras stärker de den nationella cybersäkerheten och livskraften, samtidigt som de minskar de cybersäkerhetsrisker som följer av de nuvarande bristerna eller flaskhalsarna. **Det primära målet för utvecklingsprogrammet är att i Finland skapa ett cybersäkerhetsekosystem** (bild 2) som genererar livskraft och tillväxt, ökar antalet arbetsplatser inom branschen, skapar den nödvändiga kompetensen och förbättrar det digitala samhällets hållbarhet och tålighet i förhållande till olika fenomen i cybermiljön.

Utvecklingsprogrammet går först in för fyra huvudteman som är centrala för att få ekosystemet att växa. Dessa fyra teman är: **högklassig kompetens, nära samarbete, stark finländsk cybersäkerhetsindustri och effektiva nationella cybersäkerhetskapaciteter.** Nya teman kan inkluderas under de kommande uppdateringarna av utvecklingsprogrammet.

Figur 2. Det finländska cybersäkerhetsekosystemet

3 Högklassig kompetens

Stark nationell cybersäkerhet förutsätter nödvändig kompetens och omfattande deltagande på alla olika nivåer av samhället. Aktörer som erbjuder digitala lösningar och tjänster måste kunna producera säkra tjänster. Medborgarna måste för sin del kunna använda det digitala informationssamhällets tjänster på ett säkert sätt och identifiera de risker som användningen av olika enheter, produkter och tjänster är förknippad med. Den tredje sektorns och det fria bildningsarbetets roll framhävs i arbetet för att öka medborgarnas kompetens. Samhället måste för egen del svara mot detta behov för att möjliggöra ökat förtroende.

Det finländska näringslivet, cybersäkerhetsindustrin och myndigheterna har påpekat att antalet cybersäkerhetsexperter är otillräckligt nu och under de kommande åren. Det råder ständigt hård internationell konkurrens om specialister på cybersäkerhet. Internationella experter är ofta en förutsättning för att företag inom branschen ska kunna växa, internationaliseras och ta fram nya innovationer. Specialister är även en attraktionsfaktor som lockar till sig andra specialister. Specialister behövs för att främja den finländska cybersäkerhetsindustrins, näringslivets och forskningens framgång på den globala marknaden.

De nuvarande utbildningsprogrammen genererar inte direkt den nödvändiga kompetensen för den finländska cybersäkerhetsindustrin, näringslivet och myndigheterna. Detta leder till en situation där olika aktörer även tvingas att ständigt konkurrera om samma experter och ge sin nya personal betydande vidareutbildning i samband med att arbetsuppgifterna inleds. För att säkerställa bästa möjliga genomslag ska examensstudier inom ett utbildningsprogram för cybersäkerhet planeras i samarbete med olika aktörer, och innehållet i studierna ska uppdateras regelbundet för att svara mot olika aktörers behov. Undervisning i cybersäkerhet borde vidare inkluderas i de examensstudier som skapar kompetens för teknologisektorerna. Detta främjar inbyggd säkerhet i de olika infrastrukturerna, funktionerna och tjänsterna i samhället. För att få bukt med kompetensunderskottet och säkerställa tillräckligt bred och mångsidig kompetens ska kvinnor och flickor och andra underrepresenterade grupper uppmuntras och sporras att söka sig till cybersektorn.

För att främja yrkeskunnigheten inom cybersäkerhet behövs satsningar på examensinriktad utbildning, examensinriktad fortbildning och påbyggnadsutbildning för att öka antalet cybersäkerhetsexperter inom den offentliga och den privata sektorn. Inom universitets- och yrkeshögskoleutbildningen ska biämnesutbildningen inom cybersäkerhet dessutom ökas i form av en separat studiehelhet, så att cybersäkerhetsstudier kan erbjudas även andra än studerande inom cybersäkerhetsområdet. Utvecklingsprogrammet uppmuntrar även arbetsgivare och läroanstalter till ett allt närmare samarbete till exempel när det gäller att öka antalet praktikperioder. Detta gör det lättare att tillämpa studierna inom området i arbetslivet och främjar övergången till det egentliga arbetslivet.

För att utveckla internationellt konkurrenskraftiga och säkra cybersäkerhetsprodukter och -tjänster krävs att företagen har tillgång till specialister på cybersäkerhetsteknik och cybersäkerhetsprocesser som ingående behärskar de centrala delområdena inom sektorn. För att utveckla högklassig nationell kompetens inom cybersäkerhet krävs att ett tillräckligt kompetenscenter bildas. Bildandet av ett center för högklassig kompetens kräver i sin tur ett nära samarbete mellan högskolorna nationellt och internationellt, tvärvetenskaplighet och samarbete med flera andra intressentgrupper. I utvecklingen ska engageras aktörer inom undervisnings- och utbildningssektorn (grundskolor, gymnasier, yrkesskolor, yrkeshögskolor, universitet), forskningsinstitutioner, den offentliga förvaltningen, centrala aktörer inom näringslivet och samarbetsekosystem, aktörer med anknytning till den kritiska infrastrukturen i samhället och företag och aktörer inom cybersäkerhetsbranschen. Dessutom ska man uppmuntra till att stärka och fördjupa det internationella samarbetet och skapa nära relationer till internationella center för högklassig kompetens.

3.1 Förslag till utvecklingsåtgärder

En god nivå på medborgarnas cybersäkerhetskunskaper

Organisationernas och frivilliggruppernas roll stärks i utvecklingen av medborgarnas cybersäkerhetsfärdigheter. Organisationernas roll definieras i säkerhetskommunikationsarbetet gällande medborgarnas cybersäkerhet och deras verksamhet stöds inom denna uppgift.

Ökandet av medborgarnas medvetenhet effektiviseras ytterligare som en del av den europeiska cybersäkerhetsmånaden och den nationella veckan för digital säkerhet, som samordnas av Myndigheten för digitalisering och befolkningsdata. Som en del av den nationella veckan för digital säkerhet återinförs även den nationella dataskyddsdagen. Verksamheten i cybersäkerhetssammanslutningar som bygger på frivillighet stöds, och kompetensen utnyttjas i utvecklingen av både de allmänna och de fördjupade kunskaperna.

Organisationerna stöds dessutom även i beredskapen för uppföljning av allvarliga cyberattacker samt i verkställandet av denna beredskap i samarbete med myndigheterna. Detta förutsätter en uppdatering av ansvars- och verksamhetsmodellerna samt ökade kunskaper om cyberattackers effekter och följderna av dem hos aktörer som erbjuder uppföljning.

Utöver det ovannämnda skapas dessutom en kommunikationsplan med nödvändiga åtgärder för att öka medborgarnas cybersäkerhetsmedvetenhet.

Utveckling av utbildningen inom cybersäkerhet

Vid planeringen av utbildningen i cybersäkerhet strävar man efter att beakta såväl näringslivets som den offentliga förvaltningens kompetensbehov i fråga om cybersäkerhet. I den mån det är möjligt försöker man inom förskolepedagogiken skapa grunder för barnen att förstå hur produkter och tjänster i det digitala samhället används tryggt. Man överväger att inkludera cybersäkerheten i grundskolans läroplaner utifrån en separat undersökning. Inom den allmänbildande grundläggande utbildningen strävar man efter att säkerställa att de unga har tillräckliga färdigheter att verka i en digital omvärld och att de förstår cybersäkerhetshoten och kan skydda sig mot dem.

Inom gymnasieutbildningen strävar man efter att i den mån det är möjligt utvidga och fördjupa dessa färdigheter och skapa en grund för sektorns specialkompetens inom högskoleutbildningen. Strävan är att i tillämpliga delar inkludera cybersäkerhetsfrågor i yrkesutbildningen som en del av den grundläggande yrkeskompetensen inom branschen. Målet är att säkerställa en trygg verksam-het i den digitala miljön och det kunnande som anknyter till den ska integreras i studierna på ett sätt som lämpar sig för yrkesområdet, oberoende av den som studerar och yrket. För att utveckla yrkeskompetensen och den kompletterande cybersäkerhetskompetensen strävar man efter att planera kompetensvägar där man utnyttjar redan existerande innehåll och vid behov skapar nya. Kvinnor och flickor och andra underrepresenterade grupper uppmuntras att intressera sig för cybersektorn.

Behoven av topp- och specialkompetens identifieras och kompetensen utvecklas enligt behoven. Gemensamma cybersäkerhetsutbildningar ordnas centraliserat oberoende av sektor. Arbetet med att ta högklassiga internationella utbildningar och utbildare till Finland stöds, och relationer skapas till internationella center för högklassig kompetens. Virtuella genomföranden och andra kostnadseffektiva lösningar utnyttjas i mån av möjlighet när utbildningar ordnas.

4 Nära samarbete

Ett ännu närmare samarbete mellan i synnerhet den offentliga förvaltningen och näringslivet har identifierats som en betydande möjlighet. Detta ses som en viktig faktor i stärkandet av cybersäkerhetsekosystemet. Man vill hitta nya metoder och former för samarbetet mellan aktörerna inom det nationella cybersäkerhetsfältet. Man vill även aktivera cybersäkerhetssammanslutningar mer i den kontinuerliga förbättringen av cybersäkerheten hos statsförvaltningens digitala tjänster.

Övningsverksamheten gällande cybersäkerhet upprätthålls och främjas. Aktiv övningsverksamhet är av central betydelse för utvecklingen av bekämpningen, hanteringen och lösningen av cyberattacker. Samarbete med Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka) och projektet Digital säkerhet 2030 är viktigt för att främja dessa kapaciteter.

Utvecklingsprogrammet uppmuntrar till att öka de strategiska partnerskapsmodellerna mellan företag och universitet och högskolor. Långsiktigt samarbete bör genom forsknings- och utvecklingsarbete möjliggöra uppkomsten av nya produkt- och tjänsteinnovationer. Detta främjar kommersialiseringen av produkter och tjänster inom den finländska cybersäkerhetsindustrin.

Aktivt internationellt samarbete skapar för sin del förutsättningar för cybersäkerhetsekosystemets tillväxt och för upprätthållandet och utvecklingen av ett säkert digitalt samhälle och i bredare bemärkelse för stärkandet av säkerheten i Finland. Internationellt samarbete ses som en central möjlighet att främja bilden av ett säkert Finland och skapa enhetliga referensramar för cybersäkerhet. Att referensramarna för cybersäkerhet internationellt sett är enhetliga är ofta även ett livsvillkor för tillväxt. Samarbete möjliggör internationell jämförelse av cybersäkerhetsnivån, vilket stöder främjandet av ett säkert digitalt samhälle och utvecklingsvägen för kontinuerlig förbättring.

4.1 Förslag till utvecklingsåtgärder

Stärkande av samarbetet kring övningsverksamhet inom cybersäkerhet

Myndigheterna, näringslivet och organisationerna har ett nära samarbete kring övningsverksamhet inom cybersäkerhet för att trygga verksamheten i värdekedjor som är kritiska för samhällets funktion. Gemensamma cyberövningsmiljöer används i övningsverksamheten inom cybersäkerhet. Övningsverksamhetens kontinuitet och den tväradministrativa styrningen av dessa säkerställs. Dessutom stöds ordnandet av övningar som anknyter till EU:s cybersäkerhet och hot mot EU.

Främjande av det nationella forsknings- och utvecklingssamarbetet inom cybersäkerhet

Forsknings- och utvecklingssamarbetet inom cybersäkerhet samordnas så att de gemensamma målen uppnås. Tillgången till finländsk och internationell finansiering av cybersäkerhetsforskning främjas med beaktande av säkerhetsaspekter. Utöver de teoretiska forskningsresultaten identifieras möjligheterna att kommersialisera resultaten i större utsträckning än tidigare och främjandet av dem stöds. Forskningsverksamheten inkluderas i företagens innovations-, produkt- och tjänsteutvecklingsprocesser och i det internationella samarbetet.

Cybersäkerhetssamfundet aktiveras i större utsträckning än tidigare för att säkerställa att statsförvaltningens digitala tjänster är säkra. Samfundets kompetens kan utnyttjas till exempel för att utveckla säker programkod och i tillämpliga delar starta statsförvaltningens ”Bug Bounty”-program för kontinuerlig förbättring av de digitala tjänsternas säkerhet.

Aktivt deltagande i och påverkan av det nationella och internationella cybersäkerhetssamarbetet

Finland deltar i och påverkar aktivt utvecklingen av EU:s gemensamma utrikes- och säkerhetspolitik gällande cybersäkerhet och samarbetar för att stärka EU:s cyberfunktionsförmåga. Målet är en fri, öppen och säker cybermiljö där den demokratiska principen, mänskliga rättigheter och internationell lag respekteras. På den operativa nivån ska starkare samarbete och samverkan mellan myndigheter som ansvarar för nät- och dataskyddsfrågor (NIS), myndigheter som utövar tillsyn över lagen och säkerhetsmyndigheter samt aktörer som ansvarar för cyberdiplomati och cyberförsvar stödjas i medlemsländerna och på EU-nivå. Dessutom deltar man aktivt i internationellt cybersäkerhetssamarbete i de centrala internationella organisationerna (bl.a. inom ramen för FN, OECD, OSSE, ITU-T och Nato-partnerskapet) samt i bilaterala samarbeten.

Målet med arbetet är att göra den finländska cybersäkerhetskompetensen mer känd, bereda gemensamma cybersäkerhetskrav, standarder och utvärderingskriterier för certifiering, utbyta information och främja en gemensam finländsk cybersäkerhetsagenda som en del av den globala verksamhetsmiljön. Cybersäkerhetsindustrins deltagande i bildandet av de ovannämnda internationella samarbetsgruppernas ståndpunkt stöds genom att temabaserade samarbetsgrupper inrättas. Dessutom ska finländska aktörer effektivt kunna påverka internationella processer och internationell praxis som förbättrar cybersäkerheten i Finland.

Finlands framgång på det internationella cybersäkerhetsfältet följs upp utifrån internationella index (ITU: Global Cybersecurity Index (GCI) och e-Governance Academy: National Cyber Security Index (NCSI).

5 Stark finländsk cybersäkerhetsindustri

En stark finländsk cybersäkerhetsindustri är en av de viktigaste möjliggörande faktorerna för ett nationellt cybersäkerhetsekosystem. Cybersäkerhetsindustrin skapar kapaciteter att trygga tjänsterna i det digitala informationssamhället, bygga ekonomisk tillväxt, öka kompetensen och skapa nya arbetsplatser. Förutsättningarna för att expandera den starka inhemska cybersäkerhetsindustrin är beroende av de andra huvudtemana i det här utvecklingsprogrammet. Finland behöver fler framgångsrika cybersäkerhetsprodukter och -tjänster, nya cybersäkerhetsföretag, stöd för tillväxt och internationalisering hos de befintliga företagen och samarbete mellan olika aktörer. En stark cybersäkerhetsindustri lägger även grunden för ambitionen att det nationella cybersäkerhetsekosystemet ska bli självförsörjande.

Den växande internationella cybersäkerhetsmarknaden är en betydande möjlighet för Finland när det gäller ekonomisk tillväxt och sysselsättning. Finland ska vara en internationellt attraktiv miljö för cybersäkerhet, affärsverksamhet inom IKT-branschen och investeringar. Att internationella företag etablerar sig i Finland, gör forsknings- och produktutvecklingssatsningar i Finland och har ett fungerande samarbete med finländska aktörer är en central del av uppkomsten av ett ekosystem inom cybersäkerhetsbranschen samt av den nationella och internationella cybersäkerhetsmarknadens tillväxt.

För att utveckla en stark finländsk cybersäkerhetsindustri krävs tekniska och kommersiella kapaciteter av flera olika slag. Främjandet av dessa beaktas som en del av utvecklingsprogrammet. Stöd för grundande av nya företag, uppkomst av ny finländsk IPR (t.ex. immateriella rättigheter gällande teknologier och programvaruprodukter), alstrande och stöd av den nödvändiga kompetensen samt identifiering och utnyttjande av olika roller i det internationella ekosystemet är viktiga delfaktorer i uppbyggnaden av de kommersiella kapaciteterna. Internationell tillväxt ska också sökas för nya nationella innovationer, produkter och tjänster.

EU:s kompetenscentrum för cybersäkerhet, som grundas 2021, och det nationella samordningscentrum som ska utses i Finland och fungera som kontaktpunkt för kompetenscentrumet och en del av nätverket kommer att finansiera forskningsprojekt inom cybersäkerhet och utveckling av cybersäkerhetskompetenser. Målgruppen är framför allt små och medelstora företag. Det nationella samordningscentrumet ska ha substanskompetens inom cybersäkerhet samt förmåga att hjälpa till att samla forskningsprojekt och stödja företag i utvecklingen av inhemska produkter och tjänster som ytterligare främjar uppbyggnaden och exporten av ett nationellt cybersäkerhetsekosystem.

5.1 Förslag till utvecklingsåtgärder

Stöd för finländska cybersäkerhetsprodukters och -tjänsters tillväxt och internationalisering

Utvecklingen av en stark finländsk cyberindustri kräver tillväxt, internationalisering och investeringar. Som grund för detta utarbetas en tillväxtstrategi för cybersäkerhetssektorn för att stödja marknadens tillväxt och främja tillgången på internationella investeringar i Finland. Dessa lägger även grunden för utvecklingen av det nationella ekosystemet.

Den finländska cybersäkerhetsindustrins innovationer, produkter och lösningar utnyttjas i större utsträckning och djärvare än tidigare. Upphandlingskompetensen inom köp av cybersäkerhetsprodukter och -tjänster utvecklas. Man ser möjligheterna i försökskultur och stöder försök och kommersialisering av dem. De ovannämnda åtgärderna samordnas med åtgärderna i Nationell strategi för offentlig upphandling 2020.

Finlands beskickningar utomlands och i synnerhet nätverket Business Finland, som verkar i anslutning till dem, aktiveras i större utsträckning än tidigare till internationellt samarbete för att göra den finländska cybersäkerhetskompetensen mer känd. Det nationella utbytet av information utvecklas, så att Finlands cybersäkerhetsfördelar och intressebevakning kan drivas decentraliserat, men som en front och med ett enhetligt budskap.

Produktifieringen och konceptualiseringen av produkter och tjänster främjas med utgångspunkt i den internationella marknaden. Finlands styrkor utnyttjas i internationaliseringen och marknadsföringen. Tillgången på internationella investeringar i Finland stöds också, vilket lägger grunden för utvecklingen av det nationella ekosystemet.

Främjande av grundandet av nya cybersäkerhetsföretag

För att förverkliga en stark finländsk cybersäkerhetsindustri krävs cybersäkerhetsföretag i olika faser av livscykeln. För att detta ska vara möjligt måste man stödja utvecklingen av cybersäkerhetsföretag i olika faser av livscykeln och möjliggöra företagens uppkomst och tillväxt. Företagen behöver bättre tillgång till inhemska finansieringsinstrument som är relevanta för cybersäkerhetsindustrin och bättre tillgång till kapital, inklusive eventuella statliga finansierings- och ägarandelar.

Stödstrukturerna för framför allt små och medelstora företags cybersäkerhetskompetens ska stärkas med hjälp av de EU-finansierade nationella kluster och nätverk som ska utses 2021. I det här arbetet utnyttjas verksamheten inom EU:s kompetenscentrum och det nationella samordningscentrumet när det gäller att främja grundandet av cybersäkerhetsföretag genom att ett tillväxt- och kompetenscenter för cybersäkerhet grundas i anslutning till det nationella samordningscentrumet. Samarbetet med bl.a. Arbets- och näringsministeriet, Business Finland, Kyberala ry (FISC) och andra nödvändiga samarbetspartner fortsätter och intensifieras ytterligare, och nya försök inleds i syfte att effektivisera denna samverkan ytterligare.

6 Effektiva nationella cybersäkerhetskapaciteter

Nationella cybersäkerhetskapaciteter lägger grunden för verksamheten i hela samhället. De nationella cyberkapaciteterna omfattar även de procedurer som används för att säkerställa den nödvändiga nivån på och verksamhetsförutsättningarna för cybersäkerheten. Cybersäkerhetskapaciteterna främjar vidare vår suveränitet i cybermiljön och medborgarnas förtroende för verksamheten i det digitala samhället under alla samhälleliga förhållanden. När de nationella cybersäkerhetskapaciteterna utvecklas måste man beakta det ömsesidiga beroendet mellan olika sektorer och funktioner på både det nationella och det internationella planet samt medborgarnas beroende av centraliserade tjänster inom det digitala samhället. I den digitala miljön är det av största vikt att sekretessen, personuppgifternas integritet och konfidentialiteten bevaras.

Som en del av cybersäkerhetskapaciteterna görs en utvärdering av myndigheternas nuvarande verksamhetsförutsättningar när det gäller att säkerställa den nationella cybersäkerhetsnivån i en cybermiljö som ständigt utvecklas, samtidigt som vidareutvecklingsbehoven identifieras.

Som en del av utvecklingsprogrammet utarbetas och inleds ett åtgärdsprogram för att Finland ska kunna ansöka om att bli ett AQUA-land (Appropriately Qualified Authority) som godkänner certifiering av EU:s krypteringsprodukter senast 2027. Att erhålla AQUA-status skulle i betydande utsträckning främja de nationella krypteringskapaciteterna, hjälpa finländska företag som utvecklar högklassiga krypteringsprodukter att få tillträde till den internationella marknaden och öka det internationella förtroendet för de finländska säkerhetsmyndigheterna.

6.1 Förslag till utvecklingsåtgärder

Myndigheternas beredskap för cyberstörningssituationer ska vidareutvecklas tväradministrativt

Utredningsarbete inleds för att utvärdera myndigheternas verksamhetsförutsättningar när det gäller säkerställande av den nationella cybersäkerheten, bekämpning av cyberbrottslighet, cyberförsvar och situationer som utvecklas snabbt och som hotar cybersäkerheten i samhället med beaktande av den ständiga utvecklingen av den nationella och internationella hotmiljön. På basis av utredningsarbetet fastställer man vilka åtgärder som ska vidtas och inleder den nödvändiga lagberedningen.

Den inbyggda säkerheten i de nationella webbtjänsterna ska utvecklas

Kontrolltjänsterna för cybersäkerhet vidareutvecklas för hela samhällets bruk som en del av de inbyggda säkerhetsegenskaperna i användningen av .fi-domännamn. Inbyggda säkerhetsegenskaper av det här slaget har redan införts, men de vidareutvecklas för att svara mot det föränderliga hotläget.

Säkerhetskraven ska harmoniseras och observationsförmågan förbättras

Cybersäkerhetskraven för försörjningsberedskapskritiska sektorer och företag harmoniseras i syfte att fastställa en gemensam säkerhetsnivå, så att cybersäkerhetsrisker som följer av de ömsesidiga beroendena mellan olika sektorer kan minskas. Målet är att på så sätt öka samhällets förmåga att stå emot eventuella cyberattacker. En väsentlig del i förverkligandet av cybersäkerhetskraven och säkerhetsnivån är att trygga tillsynsmyndigheternas kompetens och resurser.

Försörjningsberedskapskritiska värdekedjor som överskrider samhällsgränserna identifieras, och lägesbilden för deras cybersäkerhet utvecklas. Kapaciteterna som anknyter till produktionen av en operativ och sektorspecifik lägesbild samt en lägesbild för tillsynsmyndigheterna utvecklas för att ytterligare förbättra lägesbilden gällande den nationella cybersäkerheten.

Det nära samarbetet fortsätter med tillsynsmyndigheterna, Försörjningsberedskapscentralen, projektet Digital säkerhet 2030 och nationella och internationella aktörer som är väsentliga för genomförandet av de övriga ovannämnda åtgärderna.

Det digitala samhällets centrala information, datalager och informationstjänster ska tryggas

De datalager, informationstjänster och informationssystem som är kritiska för samhället ska identifieras och deras funktion och säkerhet ska säkerställas. Som en del av arbetet med att utveckla nya tjänster som är kritiska för verksamheten i samhället ska det även säkerställas att tjänsterna är säkra. Dessa uppgifter främjas i samarbete med Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka) och projektet Digital säkerhet 2030.

Skapande av inhemsk krypteringsteknologi och erhållande av AQUA-status

Den nationella krypteringsproduktfamiljen ska förbättras och ett nationellt kryptostrategiarbete ska etableras. De kapaciteter som krävs för att få AQUA-status byggs upp. När det gäller kritiska cybersäkerhetsbolag ska det säkerställas att man i eventuella situationer där bestämmanderätten överförs på ett sätt som är negativt för det nationella intresset med hjälp av avtal eller befintlig lagstiftning har möjliggjort arrangemang som gör att statens intresse kan tryggas. Byggandet och genomförandet av nationella kommunikationsenheter, program och tjänster som är avsedda att trygga kritiska verksamhetsmiljöer ska stödjas. Exporten av den skapade krypteringsproduktfamiljen till den internationella marknaden ska främjas.

7 Uppföljning och rapportering

För varje utvecklingsåtgärd som läggs fram i genomförandeplanen för utvecklingsprogrammet har det fastställts mätare som stöder uppföljningen av hur åtgärden framskrider och genomförs. I samband med att en utvecklingsåtgärd genomförs samlar man regelbundet in och rapporterar data som anknyter till de fastställda mätarna.

Genomförandet av mätarna följs upp som en del av genomförandet av åtgärden samt inom ramen för styrningen av det här utvecklingsprogrammet. Cybersäkerhetsdirektören rapporterar hur utvecklingsprogrammet framskrider till Kommunikationsministeriet och Säkerhetskommittén två gånger per år. Framstegen inom utvecklingsprogrammet rapporteras även till intressentgrupperna i större omfattning genom att uppföljningstillställningar ordnas.

Åtgärderna i utvecklingsprogrammet genomförs i huvudsak inom ramen för statsbudgeten och befintliga anslag. Beslut om åtgärder som kräver ökade anslag eller har andra effekter på budgeten fattas separat inom ramen för statsfinanserna och de årliga budgeterna.

För att säkerställa att utvecklingsprogrammet är aktuellt och att inriktningen på utvecklingsåtgärderna är den rätta samordnar statens cybersäkerhetsdirektör en granskning av utvecklingsprogrammet varje år. Under denna granskning beaktas den förändrade hot- eller riskmiljön, förändringar i de internationella nätverken och andra faktorer eller trender som påverkar utvecklingsprogrammet och åtgärderna i det. Efter denna utvärdering uppdateras utvecklingsprogrammet eller dess genomförandeplan vid behov och godkänns av Kommunikationsministeriet och Säkerhetskommittén.

Bilaga 1. Utvecklingsprogrammets genomförandeplan

För samordningen av utvecklingsåtgärden ansvarar den organisation som nämns först i kolumnen 'Ansvariga'.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
0	Genomförande	Genomförande av utvecklingsprogrammet och uppföljning och rapportering av framstegen	**KM**	2021–2025	200 000 €/år	Verkställandet av utvecklingsprogrammet framskrider som planerat.
1	**En god nivå på medborgarnas cybersäkerhetskunskaper**					
1.1	Högklassig kompetens	Genomförande av en dataskyddsdag som en del av veckan för digital säkerhet	**KM**, FM	2021	Normala verksamhetsutgifter	Dagen har genomförts.
1.2	Högklassig kompetens	Definition av organisationernas roll i det nationella säkerhetskommunikationsarbetet gällande cybersäkerhet och stöd för denna uppgift	**KM**, FöM, SK-sekretariatet	2021	Normala verksamhetsutgifter	Organisationerna har en tydlig roll i säkerhetskommunikationsarbetet gällande cybersäkerhet. Organisationerna stöds utifrån sina roller.
1.3	Högklassig kompetens	Verksamheten i cybersäkerhetssammanslutningar som bygger på frivillighet stöds genom att identifiera möjliga samarbetsformer och i mån av möjlighet även stödja verksamheten ekonomiskt.	**KM**, FM, FöM, SK-sekretariatet	2021	100 000 €/år	Samarbetsformerna har identifierats. Samarbetet har inletts. Verksamheten stöds ekonomiskt.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
1.4	Högklassig kompetens	Flickor och kvinnor och andra underrepresenterade grupper uppmuntras att intressera sig för cybersektorn.	**KM**, ANM, IM, SK-sekretariatet, Kyberala ry (FISC)	2021–2024	Normala verksamhetsutgifter	Nuläget och de nödvändiga utvecklingsåtgärderna har identifierats. Utvecklingsåtgärder har genomförts. Fler kvinnor än i nuläget har sökt sig till studier och sysselsatts inom branschen.
1.5	Högklassig kompetens	Organisationerna stöds i beredskapen för uppföljning av allvarliga cyberattacker samt i verkställandet av denna beredskap i samarbete med myndigheterna.	**KM**, FöM, SK-sekretariatet	2021	Normala verksamhetsutgifter	Verksamhetsmodellen har fastställts. Beredskap har skapats.
1.6	Högklassig kompetens	Utarbetande av en kommunikationsplan för cybersäkerhetsmedvetenhet som riktas till medborgarna.	**KM**, FM, SK-sekretariatet	2021	Normala verksamhetsutgifter	En kommunikationsplan som syftar till att öka medborgarnas cybersäkerhetsmedvetenhet har utarbetats och verksamhet enligt planen har inletts.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
2	**Utveckling av utbildningen inom cybersäkerhet**					
2.1	Högklassig kompetens	Identifiering av ändringsbehoven i utbildningsprogrammen i samarbete med högskolorna.	**KM**, ANM, UKM	Tidtabellen utreds	450 000 €/ forskning	Ändringsbehoven gällande cybersäkerhetsutbildningen har identifierats.
2.2	Högklassig kompetens	I den mån det är möjligt skapas det inom förskolepedagogiken grunder för barnen att förstå hur de tryggt kan använda produkter och tjänster från det digitala samhället.	**UKM**	Tidtabellen utreds	Normala verksamhetsutgifter	Enligt utsikterna inkluderas cybersäkerhetsstudierna i planerna för förskolepedagogiken.
2.3	Högklassig kompetens	Man överväger att inkludera cybersäkerheten i läroplanen för grundskolan.	**UKM**	Tidtabellen utreds	Normala verksamhetsutgifter	Man överväger att inkludera cyberskyddsstudierna i läroplanen utifrån undersökningen.
2.4	Högklassig kompetens	I den mån det är möjligt utvidgas och fördjupas ovan nämnda färdigheter inom gymnasieutbildningen och det skapas en grund för branschens specialkompetens inom högskoleutbildningen.	**UKM**	Tidtabellen utreds	Normala verksamhetsutgifter	I den mån det är möjligt inkluderas cybersäkerhetsstudierna i läroplanen utifrån forskning.
2.5	Högklassig kompetens	I den mån det är möjligt utvidgas och fördjupas ovan nämnda färdigheter inom gymnasieutbildningen och det skapas en grund för branschens specialkompetens inom högskoleutbildningen.	**UKM**	Tidtabellen utreds	Normala verksamhetsutgifter	I den mån det är möjligt inkluderas cybersäkerhetsstudierna i läroplanen utifrån forskning.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
2.6	Högklassig kompetens	För att utveckla yrkeskompetensen och den kompletterande cybersäkerhetskompetensen strävar man efter att planera kompetensstigar där befintliga kompetensstigar utnyttjas och nya innehåll vid behov skapas.	**UKM**	Tidtabellen utreds	Normala verksamhetsutgifter	Man strävar efter att skapa studievägar för cybersäkerheten utifrån forskning.
2.7	Högklassig kompetens	Behoven av topp- och specialkompetens identifieras och kompetensen utvecklas enligt behoven.	**UKM**, KM, ANM, Kyberala ry (FISC), FöM, IM	Tidtabellen utreds	Normala verksamhetsutgifter	Behoven har identifierats och kompetensutveckling har möjliggjorts.
2.8	Högklassig kompetens	Myndigheternas gemensamma cybersäkerhetsutbildningar ordnas centraliserat.	**KM**, FöM, IM	Tidtabellen utreds	600 000 €/år	Gemensamma utbildningar har ordnats.
2.9	Högklassig kompetens	De redan identifierade metoderna genomförs, inkl. en smidigare tillståndsprocess, för att påskynda och underlätta rekryteringen av internationella cybersäkerhetsexperter till det finländska näringslivet och specialister till forsknings- och undervisningsarbetet på området.	**IM**, ANM, Kyberala ry (FISC)	2021–2025	Normala verksamhetsutgifter	Tillståndsprocesserna har gjorts smidigare. Internationella specialister har rekryterats.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
3	**Stärkande av samarbetet kring övningsverksamhet inom cybersäkerhet**					
3.1	Nära samarbete	Samarbete mellan myndigheterna, näringslivet och organisationerna i den övningsverksamhet som anknyter till tryggandet av de kritiska värdekedjorna.	**KM**, FöM, FM, FBC, SK-sekretariatet	2021–2023	Normala verksamhets-utgifter	Minst en övning per värdekedja har ordnats vartannat år.
3.2	Nära samarbete	Utnyttjande av gemensamma cyberövningsmiljöer och säkerställande av deras verksamhet samt tväradministrativ styrning	**KM**, FM, FöM, IM	2021–2025	1 mn €/år	De nödvändiga övningsmiljöerna har tagits i bruk och fyra övningar per år har ordnats.
4	**Främjande av det nationella forsknings- och utvecklingssamarbetet inom cybersäkerhet**					
4.1	Nära samarbete	Forsknings- och utvecklings-samarbetet inom cybersäkerhet samordnas, och finansiering riktas till den inhemska cybersäkerhetsforskningen för att de gemensamma målen ska uppnås.	**ANM**, UKM, KM, FöM, IM	2021–2025	1 mn €/år	En samordningsmodell har skapats. De gemensamma målen har identifierats. Finansieringen av den finländska cybersäkerhets-forskningen har tryggats.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
4.2	Nära samarbete	Åtgärder som aktiverar statsförvaltningens cybersäkerhetssammanslutningar inleds, till exempel utveckling av säker programkod och i tillämpliga delar Bug Bounty-program för kontinuerlig förbättring av cybersäkerheten hos de digitala tjänsterna.	**FM**, KM, SRK, alla ministerier	Kontinuerlig	100 000 €/ planeringsarbete	Åtgärder som aktiverar cybersäkerhetssammanslutningarna har inletts och Bug Bounty-programmen är i gång.
4.3	Nära samarbete	Möjligheterna att kommersialisera forskningsresultaten identifieras och detta stöds.	**ANM**, FM, FöM, Kyberala ry (FISC)	Kontinuerlig	Normala verksamhetsutgifter	Forskningsresultat som har lett till kommersialisering har genererats.
5	**Aktivt deltagande i och påverkan av det nationella och internationella cybersäkerhetssamarbetet**					
5.1	Nära samarbete	Man deltar aktivt i det internationella cybersäkerhetssamarbetet. Det skapas möjligheter för cybersäkerhetsindustrin att delta i beredningen av en gemensam ståndpunkt med hjälp av arbetsgrupper som tillsätts enligt temaområde.	**UM**, ANM, KM, FöM, FM, Kyberala ry (FISC)	Kontinuerlig	Normala verksamhetsutgifter	Påverkan är aktiv i alla betydande internationella samarbetsforum. Deltagandets genomslag utvärderas årligen för varje samarbetsforum.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
5.2	Nära samarbete	Finlands framgång på det internationella cybersäkerhetsfältet följs upp utifrån internationella index.	**FM**, KM, SK-sekretariatet, alla ministerier	Kontinuerlig	Normala verksamhetsutgifter	Uppföljning görs, man reagerar på resultaten och Finland klarar av att höja nivån årligen (GCI- och NCSI-indexet).
6	**Stöd för finländska cybersäkerhetsprodukters och -tjänsters tillväxt och internationalisering**					
6.1	Stark finländsk cyberindustri	För cybersäkerhetsbranschen utarbetas en tillväxtstrategi som även stöder internationella investeringar i Finland.	**ANM**, Kyberala ry (FISC)	2021	Normala verksamhetsutgifter	En tillväxtstrategi har skapats och verkställandet av den har inletts.
6.2	Stark finländsk cybersäkerhetsindustri	Den finländska cybersäkerhetsindustrins innovationer, produkter och lösningar utnyttjas i större utsträckning.	**ANM**, FM, FöM, alla ministerier, Kyberala ry (FISC)	Kontinuerlig	Normala verksamhetsutgifter	De inhemska cybersäkerhetsprodukternas och -tjänsternas marknadsandel växer varje år.
6.3	Stark finländsk cybersäkerhetsindustri	Upphandlingskompetensen inom köp av cybersäkerhetsprodukter och -tjänster utvecklas.	**FM**, ANM, FöM, Kyberala ry (FISC)	2021–2022	Normala verksamhetsutgifter	För att öka upphandlingskompetensen gällande cybersäkerhetsprodukter och -tjänster har utbildningar inriktats på detta och tillämpningsanvisningar getts.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
6.4	Stark finländsk cybersäkerhetsindustri	Finlands beskickningar aktiveras till internationellt samarbete för att främja den finländska kompetensens ryktbarhet.	**UM**, ANM, Kyberala ry (FISC)	Kontinuerlig	Normala verksamhetsutgifter	Samarbetet med beskickningarna har ökats och den finländska cybersäkerhetskompetensen har marknadsförts i vida kretsar.
6.5	Stark finländsk cybersäkerhetsindustri	Det nationella utbytet av information utvecklas, så att Finlands cybersäkerhetsfördelar och intressebevakning kan drivas decentraliserat, men som en front och med ett enhetligt budskap.	**UM**, ANM, FöM, Kyberala ry (FISC)	Kontinuerlig	Normala verksamhetsutgifter	Organisationer som deltar i olika internationella samarbetsforum har effektiviserat det ömsesidiga utbytet av information.
6.6	Stark finländsk cybersäkerhetsindustri	Produktifieringen och konceptualiseringen av produkter och tjänster stöds med den internationella marknaden som utgångspunkt.	**ANM**, Kyberala ry (FISC)	Kontinuerlig	Normala verksamhetsutgifter	Verksamhetsmodeller för produktifiering och marknadsföring har utvecklats och ett tillväxtkoncept som syftar till internationalisering finns tillgängligt.
6.7	Stark finländsk cybersäkerhetsindustri	Finlands styrkor utnyttjas i internationaliseringen och marknadsföringen.	**Alla ministerier,** Kyberala ry (FISC)	Kontinuerlig	Normala verksamhetsutgifter	En gemensam agenda och målsättningar har skapats och Finlands styrkor främjas aktivt på de internationella arenorna.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
6.8	Stark finländsk cybersäkerhetsindustri	Ett tillväxt- och kompetenscenter för cybersäkerhet grundas.	**ANM**, Kyberala ry (FISC), det nationella samordningscentrumet	2021–2023	Normala verksamhetsutgifter	Tillväxt- och kompetenscentrets arbete har främjat tillväxten, kompetensen och den internationella konkurrenskraften hos företag inom cyberindustrin.
7	**Främjande av grundandet av nya cybersäkerhetsföretag**					
7.1	Stark finländsk cybersäkerhetsindustri	Uppkomsten, utvecklingen och tillväxten av cybersäkerhetsföretag i olika faser av livscykeln stöds.	**ANM**, Kyberala ry (FISC), det nationella samordningscentrumet	2021–2025	Normala verksamhetsutgifter	Ett koncept (livscykelmodell) som möjliggör nya företag samt nationell och internationell tillväxt har skapats, kommunicerats och genomförs aktivt.
7.2	Stark finländsk cybersäkerhetsindustri	Företagen behöver även inhemsk finansiering och kapital, inklusive eventuella statliga finanserings- och ägarandelar.	**ANM**, SRK, KM, Kyberala ry (FISC), det nationella samordningscentrumet	Kontinuerlig	Normala verksamhetsutgifter	Tillräckligt med nationellt kapital står till buds för att möjliggöra tillväxt.
7.3	Stark finländsk cybersäkerhetsindustri	Samarbetet med bl.a. Business Finland, Kyberala ry och andra nödvändiga samarbetsparter fortsätter och intensifieras ytterligare.	**ANM**, FM, Kyberala ry (FISC)	Kontinuerlig	Normala verksamhetsutgifter	Samarbetet har lett till att internationaliseringsgraden har ökat.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
7.4	Stark finländsk cybersäkerhetsindustri	Innovativiteten hos och försöken med cybersäkerhetsrelaterade offentliga upphandlingar utvecklas i samarbete med Arbets- och näringsministeriets projekt Keino med beaktande av FUI-upphandlingar.	**ANM**, KM, FM, FöM, Kyberala ry (FISC)	2021–2022	Normala verksamhetsutgifter	Försöken och de innovativa upphandlingarna har ökat och samarbetet med projektet Keino pågår.
7.5	Stark finländsk cybersäkerhetsindustri	Ett pilotprojekt inleds inom delområdet cybersäkerhet i samarbete med Arbets- och näringsministeriets projekt Keino och kompetenscentren för investeringar i samhällsutveckling.	**ANM**, KM, FM, Kyberala ry (FISC)	2021–2024	Normala verksamhetsutgifter	Pilotprojektet har genomförts.
8	**Myndigheternas beredskap för omfattande cyberstörningssituationer ska vidareutvecklas tväradministrativt**					
8.1	Effektiva nationella cybersäkerhetskapaciteter	Ett utredningsarbete inleds för att utvärdera myndigheternas verksamhetsförutsättningar beträffande säkerställande av cybersäkerheten, bekämpning av cyberbrottslighet samt cyberförsvar.	**IM och FöM**, andra nödvändiga instanser	2021–2023	Kompletteras när utredningsarbetet är klart.	På basis av utredningsarbetet fastställer man vilka åtgärder som ska vidtas och inleder den nödvändiga lagberedningen.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
9	**Den inbyggda säkerheten i de nationella webbtjänsterna ska utvecklas**					
9.1	Effektiva nationella cybersäkerhetskapaciteter	Kontrolltjänsterna för cybersäkerhet vidareutvecklas för hela samhällets bruk som en del av de inbyggda säkerhetsegenskaperna i användningen av .fi-domännamn.	**KM**	2021–2022	Normala verksamhetsutgifter	Nya säkerhetsegenskaper har införts i mån av möjlighet.
10	**Säkerhetskraven ska harmoniseras och observationsförmågan förbättras**					
10.1	Effektiva nationella cybersäkerhetskapaciteter	En gemensam miniminivå fastställs för cybersäkerhetskraven inom de försörjningsberedskapskritiska sektorerna, inkl. företagen.	**FBC**, alla ministerier	2021–2022	Normala verksamhetsutgifter	En gemensam miniminivå har identifierats och införts inom olika sektorer.
10.2	Effektiva nationella cybersäkerhetskapaciteter	Försörjningsberedskapskritiska värdekedjor som överskrider samhällsgränserna identifieras och lägesbilder över cybersäkerheten utvecklas för dessa värdekedjor.	**FBC**	Kontinuerlig	Normala verksamhetsutgifter	Värdekedjorna har identifierats och lägesbildskapaciteterna har utvecklats så att de motsvarar behoven.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
10.3	Effektiva nationella cybersäkerhetskapaciteter	Kapaciteterna som anknyter till produktionen av en operativ och sektorspecifik lägesbild samt en lägesbild för tillsynsmyndigheterna utvecklas för att förbättra lägesbilden över den nationella cybersäkerheten.	**FBC**, KM, de sektorspecifika NIS-myndigheterna	Kontinuerlig	Normala verksamhetsutgifter	Ett gemensamt mål har satts upp för de branschspecifika tillsynsmyndigheternas lägesbildskapaciteter, kapaciteterna har identifierats, verksamheten har utvecklats och kontinuerlig verksamhet pågår.
11	**Det digitala samhällets centrala information, datalager och informationstjänster ska tryggas**					
11.1	Effektiva nationella cybersäkerhetskapaciteter	De datalager, informationstjänster och informationssystem som är kritiska för samhället ska identifieras och deras funktion och säkerhet ska säkerställas.	**FM**, FBC	Kontinuerlig	200 000 €/ utredningsarbete	Datalagren, informationstjänsterna och informationssystemen har identifierats, och tillgången till dem och deras säkerhet har säkerställts under hela livscykeln (utveckling, produktion, nedläggning).
11.2	Effektiva nationella cybersäkerhetskapaciteter	Som en del av arbetet med att utveckla nya tjänster som är kritiska för verksamheten i samhället ska det säkerställas att tjänsterna är säkra.	**FBC**, FM	Kontinuerlig	Normala verksamhetsutgifter	En säker programutvecklingsprocess har skapats för de tjänster som är kritiska för verksamheten i samhället, och processen utvecklas och efterlevs. Innan tjänsterna tas i bruk säkerställs det att de är försedda med adekvat, inbyggd säkerhet.

Identifikationskod	Tema	Utvecklingsåtgärd	Ansvariga	Tidsplan	Finansiering	Indikatorer
12	**Skapande av inhemsk krypteringsteknologi och erhållande av AQUA-status**					
12.1	Effektiva nationella cybersäkerhetskapaciteter	Den nationella krypteringsproduktfamiljen förbättras och kryptostrategiarbete etableras.	**KM**, Kyberala ry (FISC), FöM	2021–2026	2 mn €/år	Den nationella krypteringsproduktfamiljen är färdig.
12.2	Effektiva nationella cybersäkerhetskapaciteter	De kapaciteter som krävs för att få AQUA-status byggs upp.	**KM**, Traficom, VTT	2021–2026	1 mn €/år	De nödvändiga kapaciteterna har byggts upp.
12.3	Effektiva nationella cybersäkerhetskapaciteter	Cybersäkerhetsbolag som är kritiska för den nationella säkerheten identifieras och det säkerställs att man i eventuella situationer där bestämmanderätten överförs på ett sätt som är negativt för det nationella intresset med hjälp av avtal eller befintlig lagstiftning har möjliggjort arrangemang som gör att statens intresse kan tryggas.	**ANM**, SRK, FM, KM, FBC	Kontinuerlig	Normala verksamhetsutgifter	De nationellt kritiska cybersäkerhetsbolagen har identifierats och ägarandelarna har säkerställts.

Bilaga 2. Effektivitetsanalys av utvecklingsåtgärderna

ID	Tema	Utvecklings-åtgärd	Nuläge	Målbild	Konsekvenser	Bedömning av helhetseffek-terna	Föreslagna uppgifter för att genomföra åtgärden
0	Genom-förande	Genomförande av utvecklings-programmet	Utvecklingsprogrammet beskriver åtgärderna för att förbättra helhetsläget i fråga om den nationella cybersäkerheten.	Utvecklingsprogrammet genom-förs planenligt enligt tidtabellen. Utvecklingsprogrammet utvärderas regel-bundet och uppdateras för att motsvara den föränderliga helhetssituationen. Årligt investeringsbehov 200 000 €	Nationell	Mycket stor	* Planenligt genomförande av utvecklings-programmet. * Regelbunden utvärdering och uppdatering av utvecklingsprogrammet.
1	Högklassig kompetens	En god nivå på medborgarnas cybersäkerhets-kunskaper	Medborgarfärdigheterna inom cybersäkerhet lig-ger inte på tillräckligt hög nivå i förhållande till de nuvarande kraven som digitaliseringen ställer.	Målbilden är att varje medborgare, från barn till pensionärer, ska ha tillräckliga färdigheter för att verka i det digitala samhället. Med en riktad investering på 100 000 €/år för att stödja sammanslutningarna kan man bl.a. säkerställa att de nödvändiga praktiska kostnaderna täcks. Detta anses ha betydande inverkan på säkerställandet av kontinuiteten i verksamheten.	Internationell	Stor	* Genomförande av en cybersäkerhetsdag som en del av veckan för digital säkerhet * Definition av organisationernas roll i det nationella säkerhetskommunikationsarbetet gällande cybersäkerhet och stöd för denna uppgift. * Verksamheten i cybersäkerhetssamman-slutningar som bygger på frivillighet stöds genom att möjliga samarbetsformer identi-fieras. Verksamheten stöds i mån av möjlig-het även ekonomiskt. * Organisationerna stöds i beredskapen för uppföljning av allvarliga cyberattacker samt i verkställandet av denna i samarbete med myndigheterna.
					Nationell	Mycket stor	
					Förvaltningsområde/ sektor	Stor	
					Organisation/företag	Mycket stor	
					Medborgare	Mycket stor	

ID	Tema	Utvecklings-åtgärd	Nuläge	Målbild	Konsekvenser	Bedömning av helhetseffekterna	Föreslagna uppgifter för att genomföra åtgärden
2	Högklassig kompetens	Utveckling av utbildningen inom cybersäkerhet	Utbildningsprogrammen inkluderar inte tillräckligt med cybersäkerhetsstudier som stöder näringslivets och samhällets behov. I nuläget förbereder utbildningsprogrammen inte experterna för de ovannämnda behoven och experterna utbildas först efter att de har trätt in i arbetslivet.	Innehållet i utbildningsprogrammen och utbildningsvägarna skulle ha planerats så att utbildningsprogrammen genererar experter som redan är mer redo för behoven i näringslivet och samhället. Dessutom skulle det finnas tillräckligt med studier som hänför sig till uppdatering av kompetensen och cybersäkerheten inom specialområden. För att genomföra detta mål krävs ett omfattande utredningsarbete, där kostnaderna uppskattas till 450 000 €. Konsekvenserna av utredningsarbetet anses mycket viktiga för utvecklingen av hela utbildningssystemet och cybersäkerhetskompetensen. Vidare skulle intensivare centralisering av myndigheternas cybersäkerhetsutbildningar än i nuläget skapa bättre möjligheter att kontinuerligt utveckla kompetensen och förverkliga den på det nationella planet. De uppskattade investeringarna för att genomföra detta uppgår till 600 000 € per år.	Internationell	Stor	* Inom förskolepedagogiken strävar man efter att skapa grunder för barnen att förstå hur de tryggt använder produkter och tjänster från det digitala samhället. På basis av undersökningen ska cybersäkerheten i mån av möjlighet inkluderas i läroplanen för grundskolan, och inom gymnasieutbildningen strävar man efter att utvidga och fördjupa dessa färdigheter och att skapa en grund för branschens specialkompetens inom högskoleutbildningen. Strävan är att i yrkesutbildningen inkludera studier som syftar till grundläggande yrkeskompetens inom cybersäkerhet. *I syfte att utveckla den yrkesmässiga och kompletterande cybersäkerhetskompetensen strävar man efter att planera kompetensvägar som utnyttjar befintliga och vid behov skapar nytt innehåll. * Behoven av topp- och specialkompetens identifieras och kompetensen utvecklas enligt behoven. * Gemensamma cybersäkerhetsutbildningar ordnas centraliserat.
					Nationell	Mycket stor	
					Förvaltningsområde/sektor	Mycket stor	
					Organisation/företag	Mycket stor	
					Medborgare	Betydande	

ID	Tema	Utvecklings-åtgärd	Nuläge	Målbild	Konsekvenser	Bedömning av helhetseffekterna	Föreslagna uppgifter för att genomföra åtgärden
3	Nära samarbete	Stärkande av samarbetet kring övnings-verksamhet inom cybersäkerhet	Övningsverksamheten inom cybersäkerhet är för närvarande splittrad och aktörerna övar var och en på egen hand och i anknytning till olika scenarion. Näringslivets och organisationernas insatser i övningsverksamheten utnyttjas i nuläget inte tillräckligt.	När det gäller övningsverksamheten inom cybersäkerhet ska ett mer intensivt samarbete än tidigare idkas, så att näringslivet är nära involverat ur ett försörjningsberedskapskritiskt perspektiv och organisationerna spelar en mer betydande roll. Gemensamma långsiktiga hotscenarion och cybersäkerhetsmiljöer utnyttjas målinriktat. Investering i gemensamma övningsmiljöer skapar visshet om att kontinuiteten säkerställs i fråga om verksamheten i miljöerna och aktualiteten. Detta ses som mycket betydelsefullt för upprätthållandet och utvecklingen av kompetensen och samarbetet. De årliga investeringarna uppskattas uppgå till 1 mn €.	Internationell	-	* Samarbete mellan myndigheterna, näringslivet och organisationerna i den övningsverksamhet som anknyter till tryggandet av de kritiska värdekedjorna. * Utnyttjande av gemensamma cyberövningsmiljöer och säkerställande av deras verksamhet.
					Nationell	Mycket stor	
					Förvaltningsområde/ sektor	Stor	
					Organisation/företag	Stor	
					Medborgare	-	

ID	Tema	Utvecklings-åtgärd	Nuläge	Målbild	Konsekvenser	Bedömning av helhetseffekterna	Föreslagna uppgifter för att genomföra åtgärden
4	Nära samarbete	Främjande av det nationella forsknings- och utvecklingssamarbetet inom cybersäkerhet	Cybersäkerhetsforskning bedrivs, men den samordnas inte för att uppå de gemensamma målen. Det finns utmaningar när det gäller kommersialiseringen av forskningsresultaten. Det finns inte tillräckligt med forskningsfinansiering.	Forsknings- och utvecklingssamarbetet inom cybersäkerhet samordnas så att de gemensamma målen uppnås. Tillräckligheten av den inhemska finansieringen av cyberforskning stöds. Utöver de teoretiska undersökningsresultaten identifieras möjligheterna att direkt kommersialisera resultaten i större utsträckning än tidigare och främjandet av dem stöds. Samfundet stöder kontinuerlig förbättring av cybersäkerheten. Det nationella cybersäkerhetsforsknings- och utvecklingsarbetet anses spela en mycket betydelsefull roll. Forskningen skapar potential för nya innovationer och tillväxt. Det årliga investeringsbehovet för detta arbete har uppskattats till 1 mn €. I aktiveringen av olika sammanslutningar ses även betydande möjligheter inom utveckling av cybersäkerheten i det digitala samhället. Aktivering av samfundet kräver gemensamma spelregler och verksamhetsmodeller. Investeringsbehoven för att förverkliga dem uppskattas till 100 000 €.	Internationell	-	* Forsknings- och utvecklingssamarbetet inom cybersäkerhet samordnas så att de gemensamma målen uppnås. * Samfundsåtgärder inleds i syfte att utveckla säker programkod för statsförvaltningen och förbättra de digitala tjänsternas säkerhet. * Tillräckligheten av den inhemska finansieringen av cyberforskning stöds. * Möjligheterna att kommersialisera forskningsresultaten identifieras och detta stöds.
					Nationell	Mycket stor	
					Förvaltningsområde/sektor	Mycket stor	
					Organisation/företag	Stor	
					Medborgare	-	

ID	Tema	Utvecklings-åtgärd	Nuläge	Målbild	Konsekvenser	Bedömning av helhetseffekterna	Föreslagna uppgifter för att genomföra åtgärden
5	Nära samarbete	Aktivt deltagande i och påverkan av det nationella och internationella cybersäkerhetssamarbetet	Alla möjligheter till nationellt och internationellt samarbete utnyttjas inte effektivt i nuläget.	Finland deltar i samarbetet med de organisationer som nämns i cybersäkerhetsstrategin, utvecklar det nationella utbytet av information och främjar det internationella samarbetet genom bl.a. ambassaderna.	Internationell	Mycket stor	* Man deltar aktivt i det internationella cybersäkerhetssamarbetet. * Finlands framgång på det internationella cybersäkerhetsfältet följs upp utifrån internationella index.
					Nationell	Mycket stor	
					Förvaltningsområde/sektor	-	
					Organisation/företag	Betydande	
					Medborgare	-	
6	Stark finländsk cybersäkerhetsindustri	Stöd för finländska cybersäkerhetsprodukters och -tjänsters tillväxt och internationalisering	Det stöd som finländska cybersäkerhetsprodukter erbjuds för i synnerhet internationalisering och tillväxt ska vidareutvecklas.	Det finns stöd och finansiering att få för en övergång från den nationella marknaden till den internationella marknaden. Finlands styrkor utnyttjas aktivt i marknadsföringen, och produktutvecklingen stöds genom det egna köpbeteendet. För den nationella cybersäkerhetsindustrin skapas en tillväxtstrategi som även beaktar internationella investeringar som riktas till Finland och som stärker cyberekosystemet.	Internationell	Mycket stor	* En tillväxtstrategi skapas för den nationella cybersäkerhetsindustrin. * Den finländska cybersäkerhetsindustrins innovationer, produkter och lösningar utnyttjas i större utsträckning. * Upphandlingskompetensen inom köp av cybersäkerhetsprodukter och -tjänster utvecklas. * Finlands beskickningar aktiveras till internationellt samarbete för att främja den finländska kompetensens ryktbarhet. * Det nationella utbytet av information utvecklas, så att Finlands cybersäkerhetsfördelar och intressebevakning kan drivas decentraliserat, men som en front och med ett enhetligt budskap. * Produktifieringen och konceptualiseringen av produkter och tjänster stöds med den internationella marknaden som utgångspunkt. * Finlands styrkor utnyttjas i internationaliseringen och marknadsföringen.
					Nationell	Mycket stor	
					Förvaltningsområde/sektor	Stor	
					Organisation/företag	Mycket stor	
					Medborgare	Betydande	

ID	Tema	Utvecklings-åtgärd	Nuläge	Målbild	Konsekvenser	Bedömning av helhetseffekterna	Föreslagna uppgifter för att genomföra åtgärden
7	Stark finländsk cybersäkerhetsindustri	Främjande av grundandet av nya cybersäkerhetsföretag	Stödet för grundande av nya cyberskyddsföretag bör vidareutvecklas i fråga om produktifiering och finansiering, med beaktande av företagens olika skeden i livscykeln.	Det finns tillräckligt med kapital och finansiering för cybersäkerhetsindustrin. Verksamheten i företag som befinner sig i olika faser av livscykeln stöds på lämpligt sätt.	Internationell	-	* Uppkomsten och utvecklingen av cybersäkerhetsföretag i olika faser av livscykeln stöds och tillväxt skapas. * Företagen behöver även inhemsk finansiering och kapital, inklusive eventuella statliga finanserings- och ägarandelar. * Samarbetet med bl.a. Business Finland, Kyberala ry (FISC) och andra nödvändiga samarbetsparter fortsätter och intensifieras ytterligare. * Innovativiteten hos och försöken med cybersäkerhetsrelaterade offentliga upphandlingar utvecklas i samarbete med Arbets- och näringsministeriets projekt Keino med beaktande av FUI-upphandlingar. * Ett pilotprojekt inleds inom delområdet cybersäkerhet i samarbete med Arbets- och näringsministeriets projekt Keino och kompetenscentren för investeringar i samhällsutveckling
					Nationell	Stor	
					Förvaltningsområde/ sektor	Stor	
					Organisation/företag	Mycket stor	
					Medborgare	Betydande	

ID	Tema	Utvecklings-åtgärd	Nuläge	Målbild	Konsekvenser	Bedömning av helhetseffekterna	Föreslagna uppgifter för att genomföra åtgärden
8	Effektiva nationella cybersäkerhetskapaciteter	Myndigheternas beredskap för omfattande cyberstörningssituationer ska vidareutvecklas tväradministrativt	Behovet av att kartlägga och vidareutveckla myndigheternas beredskap för omfattande cyberstörningssituationer har identifierats.	Myndigheternas verksamhetsförutsättningar när det gäller att säkerställa medborgarnas cybersäkerhet och i situationer som utvecklas snabbt och hotar cybersäkerheten i samhället har utretts. Utredningen utvärderar myndigheternas verksamhetsförutsättningar beträffande säkerställande av cybersäkerheten, bekämpning av cyberbrottslighet samt cyberförsvar. Utvärderingen av nuläget har mycket stor betydelse. Utvärderingsarbetet är omfattande och inbegriper i praktiken en utvärdering av alla verksamhetsförutsättningar. Att förverkliga de utvecklingsbehov som har framkommit i utvärderingen är för sin del centralt för att säkerställa effektiviteten hos denna åtgärd. Åtgärderna och investeringsbehoven preciseras när utredningsarbetet är klart.	Internationell	-	På basis av utredningsarbetet fastställer man vilka åtgärder som ska vidtas och inleder den nödvändiga lagberedningen.
					Nationell	Mycket stor	
					Förvaltningsområde/sektor	Mycket stor	
					Organisation/företag	Stor	
					Medborgare	-	

ID	Tema	Utvecklings-åtgärd	Nuläge	Målbild	Konsekvenser	Bedömning av helhetseffekterna	Föreslagna uppgifter för att genomföra åtgärden
9	Effektiva nationella cybersäkerhetskapaciteter	Den inbyggda säkerheten i de nationella webbtjänsterna ska utvecklas	Man har identifierat ett behov av att utveckla den inbyggda säkerheten i de nationella webbtjänsterna.	Webbtjänsterna har utformats så att säkerhetstjänster finns inbyggda i dem.	Internationell	-	* Kontrolltjänsterna för cybersäkerhet vidareutvecklas för hela samhällets bruk som en del av de inbyggda säkerhetsegenskaperna i användningen av .fi-domännamn.
					Nationell	Mycket stor	
					Förvaltningsområde/sektor	Mycket stor	
					Organisation/företag	Mycket stor	
					Medborgare	-	
10	Effektiva nationella cybersäkerhetskapaciteter	Säkerhetskraven ska harmoniseras och observationsförmågan förbättras	Säkerhetskraven inom de försörjningsberedskapskritiska sektorerna skiljer sig från varandra. Man har identifierat ett behov av att utveckla observationsförmågan och de kapaciteter som hänför sig till skapandet av en lägesbild.	Säkerhetskraven inom de försörjningsberedskapskritiska sektorerna har kartlagts, och det har säkerställts att en tillräcklig säkerhetsnivå uppnås med dem. De kapaciteter som hänför sig till skapandet av en operativ lägesbild existerar, så att en nationell lägesbild över cybersäkerheten kan skapas.	Internationell	-	* En gemensam miniminivå fastställs för cybersäkerhetskraven inom de försörjningsberedskapskritiska sektorerna, inkl. företagen. * Försörjningsberedskapskritiska värdekedjor som överskrider samhällsgränserna identifieras och lägesbilder över cybersäkerheten utvecklas för dessa värdekedjor. * Kapaciteterna som anknyter till produktionen av en operativ och sektorspecifik lägesbild samt en lägesbild för tillsynsmyndigheterna utvecklas för att förbättra lägesbilden över den nationella cybersäkerheten.
					Nationell	Mycket stor	
					Förvaltningsområde/sektor	Mycket stor	
					Organisation/företag	-	
					Medborgare	-	

ID	Tema	Utvecklings-åtgärd	Nuläge	Målbild	Konsekvenser	Bedömning av helhetseffekterna	Föreslagna uppgifter för att genomföra åtgärden
11	Effektiva nationella cybersäkerhetskapaciteter	Det digitala samhällets centrala information, datalager och informationstjänster ska tryggas	Man har identifierat ett behov av att kartlägga den kritiska informationen och de kritiska tjänsterna i samhället och säkerställa säkerheten i fråga om dessa.	De datalager, informationstjänster och informationssystem som är kritiska för samhället ska identifieras och deras verksamhet och säkerhet ska säkerställas. Som en del av arbetet med att utveckla nya tjänster som är kritiska för verksamheten i samhället ska det även säkerställas att tjänsterna är säkra. Dessa uppgifter främjas i samarbete med Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka) och projektet Digital säkerhet 2030. Investeringsbehoven för en separat utredning är uppskattningsvis 200 000 €.	Internationell	-	* De datalager, informationstjänster och informationssystem som är kritiska för samhället ska identifieras och deras verksamhet och säkerhet ska säkerställas. * Som en del av arbetet med att utveckla nya tjänster som är kritiska för verksamheten i samhället ska det säkerställas att tjänsterna är säkra.
					Nationell	Mycket stor	
					Förvaltningsområde/sektor	Mycket stor	
					Organisation/företag	-	
					Medborgare	Stor	
12	Effektiva nationella cybersäkerhetskapaciteter	Skapande av inhemsk krypteringsteknologi och erhållande av AQUA-status	Den inhemska krypteringsproduktfamiljen ska vidareutvecklas och export av den också till den internationella marknaden ska möjliggöras. Att AQUA-status saknas främjar varken de nationella krypteringskapaciteterna eller nya tillväxtmöjligheter.	Den nationella krypteringsproduktfamiljen vidareutvecklas. De kapaciteter som AQUA-status förutsätter byggs upp och AQUA-status erhålls. Finländsk krypteringsteknologi används nationellt och exporteras till den internationella marknaden. Vidareutveckling av den inhemska krypteringsproduktfamiljen och erhållande av AQUA-status ses som en mycket stor möjlighet. Detta förutsätter även att kryptostrategiarbete etableras. De årliga investeringskostnaderna för dessa uppskattas till 2 mn € (krypteringsproduktfamiljen) + 1 mn € (AQUA-status).	Internationell	Mycket stor	* Den nationella krypteringsproduktfamiljen förbättras. Kryptostrategiarbete etableras. * De kapaciteter som krävs för att få AQUA-status byggs upp. * Nationellt kritiska cybersäkerhetsbolag identifieras och de inhemska ägarandelarna i dem tryggas.
					Nationell	Mycket stor	
					Förvaltningsområde/sektor	Mycket stor	
					Organisation/företag	Mycket stor	
					Medborgare	Betydande	

Bilaga 3. Andra strategier, projekt och utredningar som har beaktats vid utarbetandet av utvecklingsprogrammet

- **Ett inkluderande och kunnigt Finland – ett socialt, ekonomiskt och ekologiskt hållbart samhälle**, statsminister Sanna Marins regeringsprogram 2019
- **Statsrådets principbeslut Strategi för cybersäkerheten i Finland 2019:** De tre strategiska riktlinjerna i principbeslutet är internationellt samarbete, ledning av cybersäkerhet, förbättrad samordning av planering och beredskap samt utveckling av kompetens inom cybersäkerhet. Dimensioneringen av resurser för cybersäkerheten och samarbetet förbättras av utvecklingsprogrammet för cybersäkerheten som sträcker sig över regeringsperioderna. Programmet konkretiserar de nationella riktlinjerna och gör helhetsbilden av projekt, forskning och utvecklingsprogram tydligare. För samordning av den nationella utvecklingen av cybersäkerheten inrättas en befattning som cybersäkerhetsdirektör vid Kommunikationsministeriet.
- **Förbättring av informationssäkerheten och dataskyddet inom kritiska sektorer i samhället.** Kommunikationsministeriet 2021.
- **European Union Agency for Cybersecurity (ENISA), 'Trusted and cyber secure Europe':** Målet för ENISA:s strategi är bl.a. att i samarbete med olika länder och aktörer uppnå en hög nivå på cybersäkerheten i medlemsländerna. Målet för strategin är vidare att bygga förtroende för det nätverksbaserade samhället och dess tjänster och öka resiliensen och på så sätt trygga säkerheten för både medlemsstaterna och deras medborgare.
- **Statsrådets principbeslut om digital säkerhet inom den offentliga förvaltningen:** Statsrådets principbeslut om digital säkerhet inom den offentliga förvaltningen och genomförandeprogrammet för det utgör en central del av utvecklingsprogrammet för cybersäkerheten. I det här principbeslutet fastställs utvecklingsprinciperna och de centrala tjänsterna för att främja säkerheten i den digitala miljön. Målet med principbeslutet är att skydda medborgarna, sammanslutningarna och samhället mot de risker och hot mot den övergripande säkerheten som kan riktas mot information, tjänster och samhällets verksamhet i en digital miljö.

- **Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka):** Programmet Haukka skildrar genomförandet av principbeslutet. För Haukka-genomförandeplanen har man valt 19 uppgifter med vilka man ska utveckla de centrala tjänsterna för digital säkerhet inom den offentliga förvaltningen. Genomförandeplanen stöder också den beredning och det genomförande av utvecklingsprogrammet inom cybersäkerhetsstrategin 2019 som har inletts samt bidrar till verkställandet av statsrådets beslut om målen för försörjningsberedskapen.
- **Försörjningsberedskapscentralens program Digital säkerhet 2030:** Programmet utvecklar störningståligheten och cybersäkerheten hos samhällets digitala infrastruktur och dess tjänster genom samarbetsprojekt med företag och nätverk. Programmet kompletterar för sin del innehållet och målen i utvecklingsprogrammet.
- **Statsrådets försvarspolitiska redogörelse, 2017.** Statsrådets försvarspolitiska redogörelse till riksdagen drar upp de försvarspolitiska riktlinjerna för hur Finlands försvarsförmåga ska upprätthållas, utvecklas och användas. Genom försvarsredogörelsen och verkställandet av den säkerställer man att Finlands försvarsförmåga motsvarar kraven i säkerhetsmiljön.
- **Arbets- och näringsministeriets Tillväxt genom digital säkerhet – färdplan 2019–2030:** Målet med färdplanen för tillväxt genom digital säkerhet är att främja företagsdriven utveckling, tillväxt och internationalisering med anknytning till digital säkerhet och kompetens som ett samarbete mellan företag, den offentliga sektorn och forskningsinstitut. Rapporten innehåller en gemensam målbild och framtidsbild för 2030 för branschen digital säkerhet, en beskrivning av kunskaperna inom branschen samt dess verksamhetsmiljö, temaspecifika visioner för 2030 och centrala mellanliggande mål för 2021 och 2025.
- **Teknologiska forskningscentralen VTT Ab:s forskning 'Current Level of Cybersecurity Competence and Future Development – Case Finland'** skildrar läget i fråga om den finländska cybersäkerhetskompetensen och de framtida utvecklingsbehoven.
- **Folkrätt i cybermiljön – Finlands nationella ståndpunkter.** Utrikesministeriet 2020.
- **Strategiska riktlinjer för utvecklingen av cyberförsvaret.** Försvarsministeriet 2019.
- **Ordlista om cybersäkerhet.** Säkerhetskommittén 2018.

Bilaga 4. Beredningsgrupp

Följande personer ingick i beredningsgruppen för utvecklingsprogrammet för cybersäkerheten:

- cybersäkerhetsdirektör *Rauli Paananen*, Kommunikationsministeriet, ordförande
- informationsförvaltningsråd *Tuija Kuusisto*, Finansministeriet
- dataförvaltningsdirektör *Ari Uusikartano*, Utrikesministeriet
- lagstiftningsråd *Tiina Ferm*, Inrikesministeriet
- dataförvaltningsdirektör *Mikko Soikkeli*, Försvarsministeriet
- konsultativ tjänsteman *Pentti Olin*, Försvarsministeriet
- generalsekreterare *Petri Toivonen*, Säkerhetskommittén
- generalmajor, ledningssystemchef *Mikko Heiskanen*, Försvarsmakten
- ingenjöröverste *Janne Jokinen*, Försvarsmakten
- en representant för Skyddspolisen
- arbetslivsprofessor *Martti Lehto*, Jyväskylä universitet
- professor *Juha Röning*, Uleåborgs universitet
- verksamhetsledare *Mika Susi*, Kyberala Ry
- affärsdirektör *Anssi Kärkkäinen*, Cinia Oy
- direktör för samhällsrelationer *Nina Hyvärinen*, F-Secure
- verkställande direktör *Petri Kairinen*, Nixu Oyj
- säkerhetsdirektör *Jari Pirhonen*, TietoEVRY Oyj

Twitter: @lvm.fi
Instagram: lvmfi
Facebook.com/lvmfi
Youtube.com/lvm.fi
LinkedIn: Kommunikationsministeriet

lvm.fi/sv

KOMMUNIKATIONS-
MINISTERIET

ISSN 1795-4045
ISBN 978-952-243-603-0