# Genomförandeplan för strategin för cybersäkerheten i Finland 2024-2035

*Denna genomförandeplan ska läsas parallellt med cybersäkerhetsstrategin.*

**Innehåll**



## 1. Inledning

Finlands cybersäkerhetsstrategi 2024–2035 har godkänts som statsrådets principbeslut den 10 oktober 2024. Strategins genomförandeplan beskriver de åtgärder som behövs för att uppnå målen samt ansvariga instanser och indikatorer för dessa. Genomförandeplanen godkänns i styrgruppen för projektet för utveckling av verksamhetsmodellen för statsrådets säkerhetsledning, som består av statssekreterare.

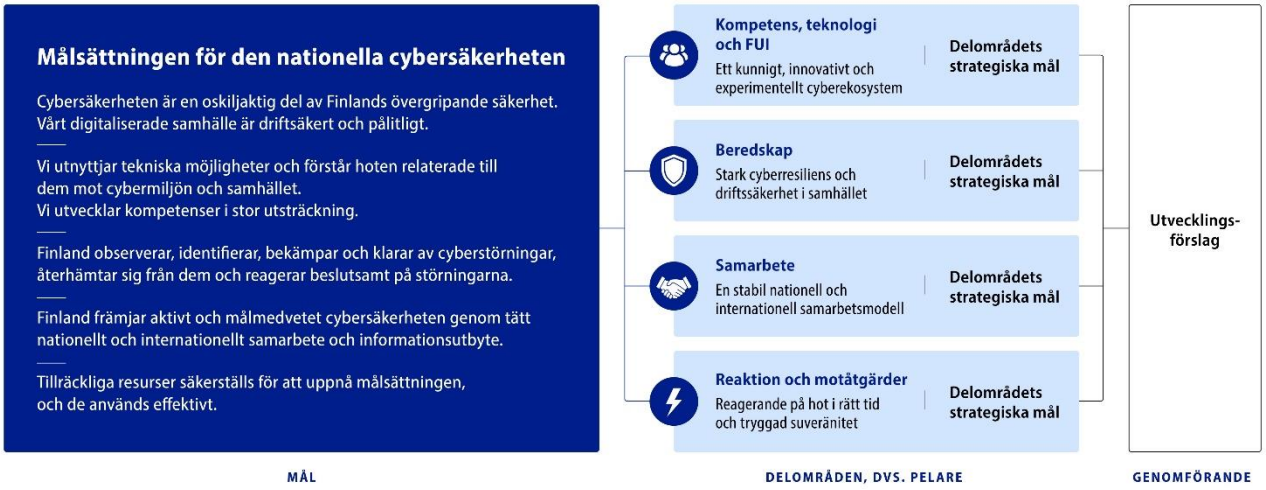
Hundratals experter, aktörer inom den offentliga och privata sektorn, forskarsamhället och medborgarorganisationer har deltagit i utarbetandet av strategin och dess genomförandeplan. Detta återspeglar det finländska samhällets engagemang och den finländska modellen för övergripande säkerhet.

Genomförandeplanen innehåller åtgärder för att uppnå målen i cybersäkerhetsstrategin. Genomförandet av planen kopplas till planeringsprocessen för de offentliga finanserna. Genomförandeplanen följs upp årligen och uppdateras vid behov. Statssekreterargruppen som fungerar som styrgrupp följer årligen upp genomförandet av strategin.

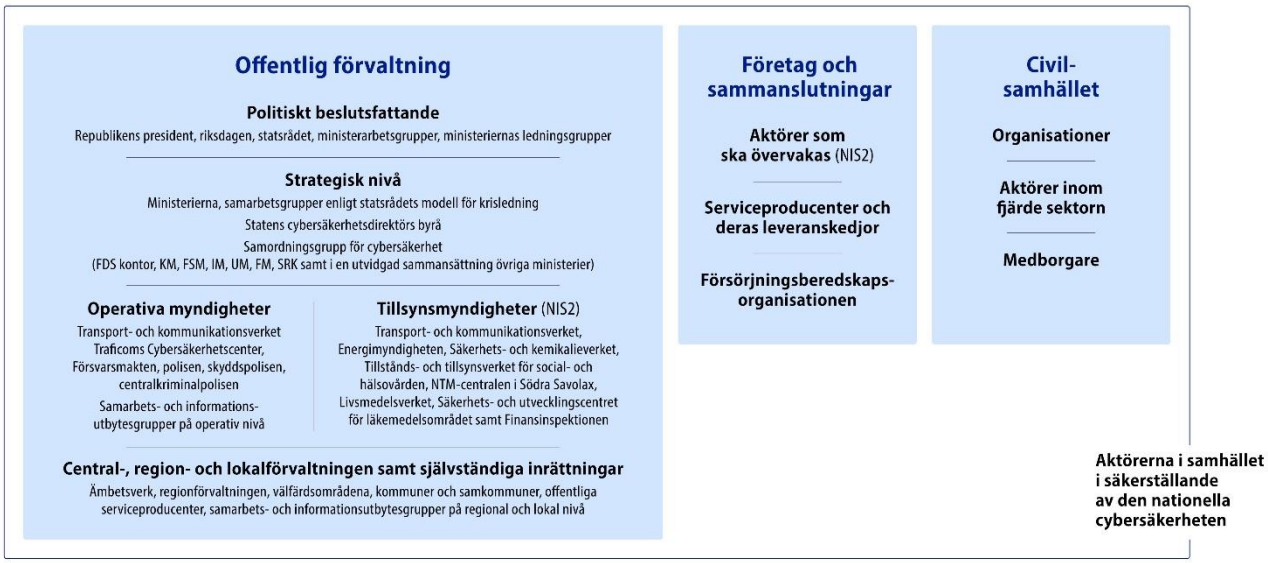
Cybersäkerhetsdirektörens byrå har huvudansvaret för att samordna uppföljningen, och uppföljningsgruppen som består av ministerierna och gruppens sekretariat stöder byrån i uppföljningen. Varje förvaltningsområde ansvarar för främjandet, finansieringen och rapporteringen av de åtgärder som har anvisats dem. Genomförandeplanen kan uppdateras årligen.

Genomförandeplanens övergripande effektivitet bedöms med hjälp av olika indikatorer, såsom nationella och internationella prestationsindikatorer för cybersäkerheten.

## 2. Cybersäkerhetsstrategins målsättning och strategins struktur




## 3. Aktörerna i samhället i säkerställande av den nationella cybersäkerheten




## 4. Genomförandeplanens struktur

Genomförandeplanen sträcker sig till 2035 och omfattar alla ovan nämnda fyra delområden eller pelare:

**I Kompetens, teknologi och forsknings-, utvecklings- och innovationsverksamhet (FUI);**
**II Beredskap;**
**III Samarbete**
**IV Reaktioner och motåtgärder.**

Genomförandeplanens struktur har kopplats till de strategiska mål och utvecklingsförslag som ingår i dessa fyra pelare. Dessa har i sin tur härletts från den målbild för den nationella cybersäkerheten som fastställts i strategin.

Åtgärderna i planen har prioriterats i två kategorier eller ”korgar”.
Korg 1 avser strategiska spetsprojekt med stor eller mycket stor genomslagskraft som man strävar efter att genomföra först.
Korg 2 innehåller projekt som genomförs på längre sikt och vars genomslagskraft inte har bedömts vara lika kritisk för närvarande.

För varje åtgärd beskrivs dess mål, tidtabell och finansiering, effektivitet samt de aktörer som deltar i genomförandet av åtgärden (**huvudsaklig ansvarig** och andra aktörer). Genomslagskraften hos varje åtgärd bedöms med hjälp av en verbal effektivitetsbedömning och på skalan nationell/internationell samt betydande/stor/mycket stor.

## 5. Verkställande och uppföljning av genomförandeplanen

Genomförandet av strategin följs upp årligen på nationell nivå. Statens cybersäkerhetsdirektörs byrå har ansvaret för att samordna uppföljningen, och förvaltningsområdena utarbetar en rapport åt byrån om genomförandet av cybersäkerheten inom sitt ansvarsområde i enlighet med tidsplanen för den offentliga ekonomins planeringsprocess. Av dessa rapporter gör byrån en sammanställning åt myndigheterna och de politiska beslutsfattarna.

Statsrådets kansli har den 1 november 2024 tillsatt en uppföljningsgrupp som ansvarar för uppföljningen och konsekvensbedömningen av genomförandet av cybersäkerhetsstrategin. Uppföljningsgruppen sammanträder ungefär kvartalsvis (februari, maj, augusti, november) eller vid behov oftare. Intressentgrupperna har möjlighet att delta i utvärderingen av strategins genomförandeplan. Intressentgrupperna hörs på våren, och det förs en aktiv dialog under året.

Förvaltningsområdena planerar och reserverar de resurser som genomförandet förutsätter och ansvarar för genomförandet av utvecklingsåtgärderna.

I uppföljningen granskas hur olika åtgärder har genomförts jämfört med strategins målbild och de utvecklingsförslag som fastställts i strategin. Rapporteringen fokuserar särskilt på vad som har åstadkommits under den gångna perioden och vad som ännu behöver utvecklas. Tyngdpunkten ligger på att rapportera konkreta resultat och det är också viktigt att berätta varför någon åtgärd inte har vidtagits.

## 5. Genomförande av uppföljningen av genomförandeplanen; ansvar

**Statssekreterarnas styrgrupp (TUJO)**
- Godkänner genomförandeplanen
- Följer upp verkställandet av genomförandeplanen årligen (uppföljningsrapport)

**Statens cybersäkerhetsdirektörs byrå**
- Samordningsansvar för uppföljningen
- Ordnar uppföljningsgruppens möten
- Ordnar årligen ett gemensamt möte med intressentgrupperna om hur genomförandeplanen framskrider

- Utarbetar en uppföljningsrapport utifrån uppföljningsgruppens svar
- Ansvarar för rapporteringen VSI OHRY, YU minry, TK (+ vid behov andra instanser)
- Uppföljningsgruppens sekretariat stöder cybersäkerhetsdirektörens byrå i uppföljningen

**Uppföljningsgruppen för cybersäkerhetsstrategin**

- Utarbetar, samordnar och uppdaterar vid behov genomförandeplanen
- Bildar en helhetsbild av förvaltningsområdenas svar
- Skickar uppgifter om framsteg till uppföljningsrapporten

**Ansvarigt förvaltningsområde/annan aktör**

- Planerar och reserverar resurser
- Utvecklar de samarbetsstrukturer som behövs för det egna ansvarsområdet
- Verkställer utvecklingsverksamheten antingen genom att ha huvudansvaret eller delta
- Rapporterar till sitt förvaltningsområde, sin sektor och uppföljningsgruppen

## 6. Genomförandeplan; åtgärder

## Pelare I: Kompetens, teknologi och FUI
## ”Ett kunnigt, innovativt och experimentellt cyberekosystem”

### Åtgärd 1.1

**Utveckling av spetskompetenser och arbetslivsfärdigheter inom den offentliga och privata sektorn samt medborgarnas och civilsamhällets cyberfärdigheter och beredskap**

**Korg 1**

**Mål**

- Utveckla kompetensen inom cybersäkerhet på alla utbildningsstadier, inom det fria bildningsarbetet, arbetskraftsutbildningarna och fortbildningarna.
- Öka effektiviteten hos och tillgången till utbildningar som främjar cybersäkerhetsfärdigheter i arbetslivet.
- Förbättra medborgarnas beredskap att agera säkert.
- Säkerställa att resultaten av projektet Cyber Citizen utnyttjas och finansiering till det.
- Skapa förutsättningar för att öka spetskompetensen genom FUI-verksamhet inom cyberbranschen
- Utöka kompetensen och tillgången till säker programutveckling.
- Utnyttja Försvarsmaktens och intressentgruppernas cyberutbildning för att öka den nationella kompetensen.
- Utveckla utnyttjandet av det frivilliga försvaret.

**Tidtabell och finansiering**

Från och med 2025
Omkostnader, till en del tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Förbättrad cybersäkerhetskompetens i samhället skapar förutsättningar för ett fungerande samhälle.

Kompetensen har förbättrats på tre nivåer: Medborgarfärdigheter, inklusive beredskap, allmänna arbetslivsfärdigheter, spetskompetens.

Utbildningarna har beaktat både kompetensbehoven, förändringarna i verksamhetsmiljön och den tekniska omvälvningen.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**UKM, KM, FSM, SRK, FBC,** Traficom, Försvarsmakten, MPK, HAUS, aktörer inom utbildningssystemet,
näringslivet.

**Åtgärd 1.2**

**Nätverkssamarbetet inom utbildningen i cybersäkerhet utvecklas**

**Korg 1**

**Mål**

- Utreda en utvidgning av nätverkssamarbetet till yrkesutbildningen och samarbetet med andra aktörer inom branschen utifrån de nuvarande nätverken för cyberkompetens vid högskolorna som leds av Jyväskylä universitet och Jyväskylä yrkeshögskola.

**Tidtabell och finansiering**

2026–2027
Tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Förbättring av samarbetet mellan utbildningsaktörerna.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**UKM**

**Åtgärd 1.3**

**Utveckla den nationella krypteringstekniska förmågan och skaffa status som land som godkänner internationella informationssäkerhetsprodukter inom EU och producerar krypteringsprodukter åt Nato**

**Korg 1**

**Mål**

- Skapa en nationell strategi, ett genomförandeprogram och en hanteringsmodell för krypteringsteknik.
- Utveckla en internationellt kompatibel nationell referensarkitektur för krypteringsteknik och en kvantsäker nationell krypteringsproduktgrupp.
- Bygga upp ett nationellt krypteringstekniskt laboratorium.
- Utveckla försörjningsberedskapen för nationella krypteringslösningar.
- Stödja exporten av krypteringsprodukter.
- Skapa/utvidga ett nationellt utbildningsprogram för krypteringsteknik och annan kompetensutveckling.

**Tidtabell och finansiering**

2025–2035
Tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Självförsörjning och försörjningsberedskap inom kritisk krypteringsteknik.
Förmågan hos aktörer som är kritiska med avseende på försörjningsberedskapen att trygga sin egen verksamhet mot krypteringstekniska hot.
Exportfrämjande stöder självförsörjningen och försörjningsberedskapen.
Förmåga att skydda kritiska nationella datalager under kvanteran.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**FSM**, ANM, KM, Traficom, Försvarsmakten, FBC, BF, Tesi, VTT, industri, högskolor

**Åtgärd 1.4**

**Kvantsäkra krypteringslösningar tas i bruk nationellt**

**Korg 1**

**Mål**

- Utarbeta en plan och anvisningar för övergång till kvantsäkra algoritmer med beaktande av riktlinjerna i den nationella kvantstrategin.
- Stödja kritiska branscher i kvantövergången.
- Bedöma behovet av att skapa skyldigheter att använda kvantresistent kryptering.

- Utnyttja modellen för innovativ offentlig upphandling.

**Tidtabell och finansiering**

2025–2035
Tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Genom att i rätt tid övergå till kvantsäkra krypteringslösningar förhindrar man att konfidentiella uppgifter äventyras eller att informationsmaterial som ska skyddas nationellt hamnar i fel händer samtidigt som man säkerställer tillgången till system och tjänster.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**KM, ANM, FM, FSM,** Försvarsmakten, Traficom, Valtori, FBC

**Åtgärd 1.5**

**Korg 1**

**Förutse och följa upp hur ny teknik och nya fenomen påverkar cybersäkerheten**

**Mål**

- Skapa en tväradministrativ modell för framtids- och prognostiseringsarbetet för cybersäkerheten.
- Producera analyserad information om framtida hot och möjligheter inom cybersäkerheten åt myndigheter och näringsliv samt utnyttja myndigheternas lägesbildsverksamhet för att dela information.
- Myndigheterna och näringslivet inleder en scenariobaserad granskning av cybermiljön.

**Tidtabell och finansiering**

Från och med 2025
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Genom att förutse cybersäkerhetsfenomen kan man identifiera framtida reglering, resursfördelning och beredskapsåtgärder samt stödja branschernas och myndigheternas beredskap inför cyberhot.

Förutsättning för utarbetande av en nationell hotbedömning.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**KM, SRK,** övriga ministerier, ämbetsverk, Traficom, FBC, näringslivet, forskningsinstitut

**Åtgärd 1.6**

**Finländska organisationers deltagande i finansieringsprogram för cybersäkerhet och nätverkssamarbete för kompetens stärks**

**Korg 2**

**Mål**

- Påverka arbetsprogrammen inom EU:s finansieringsprogram och stärka möjligheterna för finländska företag, högskolor och forskningsinstitut att delta i finansieringsprogram.
- Säkerställa tillräcklig medfinansiering för att kunna delta i projekt.
- Främja nationella aktörers anslutning till EU:s kompetensgemenskap för cybersäkerhet och möjligheter till exportfrämjande.
- Upprätthålla och utveckla den nationella utbildnings- och forskningsgemenskapen och stödja finländska aktörer att hitta nationella och internationella partner för internationella projekt.
- Producera en lägesbild av forskningen inom cybersäkerhet och finansieringen för den.

**Tidtabell och finansiering**

2025–2029
Tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Genom åtgärden kan man främja utvecklingen av nationella innovationer, forskning och kompetens inom cybersäkerhet.

Utnyttjandet av tillgänglig finansiering från EU och Nato på nationell nivå förbättras och tillväxt skapas inom cybersäkerhetsbranschen.

Den tekniska självförsörjningen främjas.

Det nationella ekosystemet för cybersäkerhet och ekosystemets internationella konkurrenskraft stärks, affärs- och exportmöjligheterna inom branschen förbättras.

Effektivitet: nationell och internationell/stor.

**Ansvarar**/aktörer

**KM, FSM, ANM, UKM, SRK,** UM, Traficom, FBC.

**Åtgärd 1.7**

**Den nationella försvarsindustrin utvecklas och stöds i innovationen och utnyttjandet av försvarsteknologi, omvälvande teknik och produkter med dubbla användningsområden samt i beredskapen inför hot**

**Korg 1**

**Mål**

- Slutföra och produktifiera bland annat projekt för säker kommunikation i indirekt industriellt samarbete inom F35-projektet.
- Etablera verksamheten vid de nationella centren och företagsacceleratorerna inom Natos DIANA-program.
- Effektivisera utnyttjandet av utvecklingsfinansiering från EU och Nato.
- Utnyttja civil finansiering effektivt när det gäller produkter med dubbla användningsområden.
- Utarbeta strategiska riktlinjer för cyberskydd inom försvars- och säkerhetssektorn och inrätta ett samarbetsnätverk för cybersäkerhet (ISAC).
- Utveckla gemensamma tjänster och responsförmåga för försvars- och säkerhetssektorn.
- Stärka det inhemska ägarskapet i företag inom cybersäkerhetsbranschen som är kritiska med tanke på försörjningsberedskapen.

**Tidtabell och finansiering**

Från och med 2025
Omkostnader, till en del tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Åtgärdernas effektivitet bedöms bland annat genom följande indikatorer:

- nationell landsprofil inom omvälvande teknik
- nationell nivå på FUI-finansieringen
- användningsgrad för inhemska kritiska lösningar inom spetsteknologi,
- självförsörjning och inverkan på försörjningsberedskapen,
- ökad exportpotential och exportvärde,
- utnyttjande av lösningar som uppfyller internationella krav utomlands,
- användningsgrad för nationella lösningar,
- nationell medfinansiering (belopp, tid), och
- nivå på cyberskyddet inom försvars- och säkerhetssektorn.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**FSM, ANM, Försvarsmakten, VTT**, BF, Tesi, industrin

**Åtgärd 1.8**

**Cybersäkerhetskompetensen utvecklas tillsammans med organisationer och näringsliv**

**Korg 1**

**Mål**

- Tillsammans med näringslivet och organisationer inleda ett projekt som främjar en förbättring av medborgarnas cybersäkerhetsfärdigheter.
- Förbättra samarbetet mellan myndigheterna och organisationsfältet i fråga om informationsutbyte och kommunikation om hot mot medborgare och olika befolkningsgrupper.
- Utvecklingen av organisationernas egen cyberförmåga stöds.
- Verksamheten vid Finnish Safer Internet Centre (FISIC) stärks.

**Tidtabell och finansiering**

2025–2027
Omkostnader, till en del tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Medborgarnas förmåga att agera tryggt i samhället stärks.
Finländarnas benägenhet att förlora pengar genom bedrägerier minskar och förtroendet för det digitala samhället stärks.

Via organisationer och näringsliv förmedlas myndighetsmeddelanden om cybersäkerhet för att stärka medborgarnas kompetens. Medborgarna kan förbereda sig på störningar i det digitaliserade samhället.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**KM, UKM**, Kavi, Traficom, FBC, näringslivet, organisationer

**Åtgärd 1.9**

**Utbildningen i bekämpning av cyberbrott utvecklas**

**Korg 2**

**Mål**

- Utveckla utbildningen i bekämpning av cyberbrott i fråga om datanätsbrott och datanätsassisterade brott. Till utvecklingen hör projektet Kyberosake som inletts tidigare samt ett projekt om kompetens inom bekämpning av datanätsassisterade brott.

**Tidtabell och finansiering**

Från och med 2024
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Behovet av kompetensutveckling har identifierats inom polisen och hos andra säkerhetsmyndigheter. Genom en utbildning som Polisyrkeshögskolan erbjuder säkerställs tillräcklig kompetens inom polisen, och utbildningen stöder även andra säkerhetsmyndigheters verksamhet.

Utöver säkerhetsmyndigheterna har även bland annat åklagare och domare möjlighet att delta i utbildningarna som ordnas av Polisyrkeshögskolan.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**IM,** Polisstyrelsen, Polisyrkeshögskolan

## Pelare II: Beredskap
## ”Stark cyberresiliens och driftsäkerhet i samhället”

**Åtgärd 2.1**

**En nationell bedömning av cyberhot utarbetas som stöd för beredskapsarbetet**

**Korg 1**

**Mål**

Utifrån scenarioarbete regelbundet utarbeta nationella hotbedömningar av cybersäkerheten för myndigheter, offentlig förvaltning och näringsliv.
Öka tillgången till och användbarheten av nationella hotbedömningar.

**Tidtabell och finansiering**

Från och med 2025
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Situationsmedvetenheten om cyberhot och fenomen som påverkar cybersäkerheten förbättras. Förutsättningarna för branschernas beredskap, riskhantering och klassificering av kritiskhet förbättras.

Den delade lägesbilden av cybersäkerheten stärks.

Hotbedömningen stöder utarbetandet av den nationella cyberkrishanteringsplan som NIS2 förutsätter och i den har kraven i CER-direktivet beaktats.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**KM, SRK, IM, FSM,** Traficom, Försvarsmakten, Skypo, övrig offentlig förvaltning, näringslivet, FBC

**Åtgärd 2.2**

**Cyberförsvaret samordnas med totalförsvaret**

**Korg 1**

**Mål**

- Identifiera och hantera cyberförsvarets inkorporering i totalförsvaret, resiliensåtgärderna och värdlandsstödet.
- Beakta det militära försvaret och den militära krisen i hanteringen av cyberkriser samt utveckla den civila sektorns beredskap och svar på dessa.
- Integrera lokalt cyberförsvar i verksamhetsmodellerna och beredskapen på lokal och regional nivå.
- Myndigheterna har förmåga att stödja kritiska aktörer.
- Utveckla uppföljningen av totalförsvarets resurser för cyberförsvarets del.

**Tidtabell och finansiering**

2025–2032
Försvarsbudget
Omkostnader, till en del tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Vi gör det möjligt för oss själva och våra allierade att operera och stödja operationer.

Nödvändiga responssystem har tagits i bruk och aktuella beredskapsplaner och avtal har ingåtts.

Militära hot och användning av maktmedel har beaktats i riskhanteringsplanen.

Uppföljning av myndigheternas och aktörernas resurser inom den civila sektorn, identifiering och hantering av riskerna med underskott i resurserna som en del av styrningen av totalförsvaret.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**FSM,** Försvarsmakten, övriga förvaltningsområden, den civila sektorn

**Åtgärd 2.3**

**Cybersäkerhet beaktas i nationella lagstiftningsprojekt**

**Korg 2**

**Mål**

Uppdatera anvisningen om konsekvensbedömning vid lagberedning.

**Tidtabell och finansiering**
2025–2027
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Den nationella lagstiftningen beaktar cybersäkerhetsaspekter och svarar på förändringar i verksamhetsmiljön.

Cybersäkerhetsaspekterna beaktas i ministeriernas lagberedning och konsekvensbedömningar av lagstiftning.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**JM**, övriga ministerier

**Åtgärd 2.4**

**Den offentliga förvaltningens cybersäkerhetsresurser planeras och följs upp långsiktigt**

**Korg 2**

**Mål**

- Planera och följa upp statens, välfärdsområdenas och kommunernas resurser för cybersäkerhet samt riskbaserad allokering av resurser.
- Bland annat MDB:s helhetsbild av den digitala säkerheten utnyttjas.

**Tidtabell och finansiering**

2025–2030
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Resurserna för cybersäkerhet inom den offentliga förvaltningen måste i tillräcklig utsträckning vara kända för att kunna säkerställa ändamålsenliga resurser och använda dem effektivt.

Användningen av resurser för att säkerställa och rikta cybersäkerheten effektiviseras bland annat med hjälp av prioritering av uppgifter och anvisningar.

Effektiviteten mäts genom att utnyttja helhetsbilden för den digitala säkerheten och anvisningarnas funktion.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**Ministerierna**, MDB, övrig offentlig förvaltning

**Åtgärd 2.5**

**Ett enhetligt verkställande av cybersäkerhetslagen säkerställs**

**Korg 1**

**Mål**

- Stärka samarbetet och samverkan mellan tillsynsmyndigheterna för NIS2 och dataombudsmannen.
- Förbättra rådgivningen och anvisningarna till branscherna om verkställandet av cybersäkerhetslagen och lagen om informationshantering inom den offentliga förvaltningen.
- Utarbeta en plan för hantering av storskaliga cybersäkerhetsincidenter och cybersäkerhetskriser.
- Förbättra dataombudsmannens verksamhetsförutsättningar.

**Tidtabell och finansiering**

2025–2029
Omkostnader, till en del tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

NIS2-direktivet är en central bestämmelse om cybersäkerhet som förenhetligar cybersäkerhetskraven inom kritiska branscher och ökar den nationella resiliensen.

Genom samarbete mellan tillsynsmyndigheterna kan man förenhetliga förfarandena och effektivisera resursanvändningen.

Genom gemensamma anvisningar kan verkställandet av lagen förbättras och effektiviseras i organisationerna.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**KM, JM,** FM, Traficom, dataombudsmannen, tillsynsmyndigheterna för NIS2

**Åtgärd 2.6**

**Aktivt påverka internationella standarder för cybersäkerhet**

**Korg 2**

**Mål**

- I stor utsträckning påverka arbetet med att standardisera cybersäkerheten i internationella organisationer.
- Införa gällande standarder proaktivt.
- Utveckla den privata sektorns delaktighet i den internationella standardiseringen.

**Tidtabell och finansiering**

Från och med 2025
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Säkerställa att nationella aspekter beaktas i tillräcklig utsträckning i beredningen av standarderna.
Den privata sektorn har beredskap och förmåga att tillämpa standarder.
Deltagandet i standardiseringsarbetet kan utnyttjas i FUI-verksamheten.

Effektivitet: nationell och internationell/stor.

**Ansvarar**/aktörer

**KM, FSM,** övriga ministerier, Traficom, Försvarsmakten

**Åtgärd 2.7**

**Uppdatering av lagstiftningen om bedömning av överensstämmelse med kraven i fråga om informationssystem, tjänster och säkerhetskritiska produkter samt utveckling av utvärderingsverksamheten i anslutning till organisationernas verksamhet och informationssystem**

**Korg 1**

**Mål**

- Förbättra tillgången till utvärdering och myndighetssamarbetet genom att granska myndigheternas utvärderingsuppgifter.
- Förbättra förutsättningarna för näringsverksamhet hos tillverkare och bedömningsorgan för säkerhetskritiska produkter i enlighet med arbetsgruppens slutrapport.
- Göra bedömningsförfarandena smidigare utifrån riskerna samt förtydliga och komplettera bedömningsgrunderna.
- Utveckla och förenhetliga bedömningskriterierna och de anvisningar och verktyg som stöder användningen av dem samt tekniska och automatiska metoder.
- Försvarsmaktens förmåga och behörighet att utvärdera och godkänna sina egna informationssystem och krypteringslösningar nationellt och internationellt uppnås.
- Utveckla certifieringen och de väsentliga kraven inom social- och hälsovårdssektorn med stöd av lagen om kunduppgifter.

**Tidtabell och finansiering**

2024–2027
Omkostnader, till en del tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

På grund av förändringarna i verksamhetsmiljön är det nödvändigt att uppdatera bestämmelserna på det sätt som beskrivs i överensstämmelsebedömningen av informationssystem för offentlig förvaltning
som utarbetats av en arbetsgrupp vid finansministeriet 2024.

Försvarsmakten och Valtori har förmåga till oberoende utvärderingsverksamhet, och den privata sektorns förmåga att bedöma och stöda utvärderingar har utvecklats.

En infrastruktur som stöder utvärdering och godkännande av informationssystem inom säkerhetskritiska branscher har byggts upp. Resursbehovet preciseras i samband med lagberedningen.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**FM, KM, FSM, SHM,** övriga ministerier, Försvarsmakten, cybersäkerhetsdirektören, Traficom, Valtori, godkända bedömningsorgan, övriga utvärderingsmyndigheter, övrig offentlig förvaltning

**Åtgärd 2.8**

**Cybersäkerhetsövningarna utvecklas så att de motsvarar den förändrade verksamhetsmiljön för att öka samhällets resiliens och trygga totalförsvarets verksamhetsförutsättningar**
**Korg 1**

**Mål**

- Trygga kontinuiteten i de nationella cybersäkerhetsövningarna.
- Göra den nationella cyberövningsverksamheten mångsidigare och öka antalet deltagare.
- Den nationella cyberövningsverksamheten svarar på totalförsvarets behov.
- Uppdatera scenarierna för övningarna.
- Utveckla sektor- och branschspecifika övningar och övningar mellan branscher, inklusive intressentgrupper.
- Övningsmaterialet utnyttjas i stor utsträckning inom olika branscher.
- Utveckla övningsmiljöerna så att de motsvarar cyberhotlandskapet bland annat genom att utnyttja EU-finansiering.
- Skapa övningsmöjligheter på strategisk nivå.
- Man deltar i multinationella (Nato och EU) cyberövningar och kan genomföra multinationella cyberövningar i Finland.

**Tidtabell och finansiering**

2026–2030

Tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Mångsidig övningsverksamhet som riktar sig till både den offentliga förvaltningen och den privata sektorn främjar starkt samhällets cyberresiliens och kompetens.

Nationella beredskaps- och cyberövningar stöder också cyberförsvarets beredskap och utveckling.

Civila aktörer och militära aktörer övar regelbundet tillsammans.

Cyberövningarna gör det möjligt att utveckla verksamheten mellan olika verksamhetsnivåer och myndigheter.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**KM, cybersäkerhetsdirektören, FBC, SRK, FSM,** övriga ministerier, Traficom, Försvarsmakten, MDB, näringslivet, organisationer, särskilt MPK

**Åtgärd 2.9**

**Säkerställa att de kommunikationsförbindelser och den tillgång till data som samhället behöver fungerar, att de har korrigeringsförmåga och att det vid behov finns alternativa kontaktsätt vid allvarliga incidenter**

**Korg 1**

**Mål**

- Säkerställa internationella datakommunikationsförbindelser med tanke på försörjningsberedskapen.

**Tidtabell och finansiering**

2025–2027
Utvecklingen sker som en del av FBC:s program DT2030.

**Konsekvensbedömning och effektivitetsanalys**

Att internationella datakommunikationsförbindelser fungerar i alla situationer är en förutsättning för att trygga försörjningsberedskapen.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**FBC, KM,** Traficom, näringslivet

**Åtgärd 2.10**

**Man identifierar specialbehoven inom cybersäkerheten inom olika sektorer i samhället och utvecklar lösningar för beredskap inför och återhämtning från incidenter**

**Korg 1**

**Mål**

- Kontinuitets-och beredskapsförfarandena hos olika sektorer i samhället och kommunala aktörer är aktuella och används.
- Aktörerna inom sektorerna och kommunsektorn har tillgång till utbildningsmaterial om cybersäkerhet och digital säkerhet som stöder den kompetens hos den högsta ledningen och personalen som behövs i cyberberedskapen.

**Tidtabell och finansiering**

2025–2027
Utvecklingen sker som en del av FBC:s program DT2030.

**Konsekvensbedömning och effektivitetsanalys**
Alla branscher är beroende av den digitala infrastrukturen och de tjänster som fungerar på den. Syftet med verksamheten är att förbättra den branschspecifika cybersäkerheten inom branscher som är kritiska för försörjningsberedskapen.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**FBC,** Traficom, näringslivet

**Åtgärd 2.11**

**Upprätthålla och stödja förmågan hos dem som producerar digital infrastruktur att förbereda sig på cyberstörningar**

**Korg 2**

**Mål**

- Stödja möjligheterna för teleföretag och producenter av digital infrastruktur att förbereda sig på cyberhot i den förändrade verksamhetsmiljön.
- Främja samarbetet mellan myndigheter och teleaktörer i frågor som gäller utvecklingen av mobilnät.

**Tidtabell och finansiering**

Från och med 2024
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Genom förtroligt samarbete i rätt tid kan man göra aktörerna inom den digitala infrastrukturen bättre på att förbereda sig på cyberhot och tekniska omvälvningar.

Genom samarbete kan man på förhand identifiera och förebygga säkerhetshot mot ny kommunikationsteknik och genom internationellt samarbete bidra till att stärka säkerheten i kommunikationsinfrastrukturen.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**KM**, Traficom, FBC

**Åtgärd 2.12**

**Förbättra resiliensen i markbundna system med hjälp av rymdtjänster**

**Korg 2**

**Mål**

- Identifiera den samhällskritiska infrastrukturens beroende av rymdtjänster.
- Säkerställa att radiofrekvenser är tillgängliga för den finländska markstations- och satellitaffärsverksamheten.
- Förbättra resiliensen i markbundna system genom att rymdtjänster utnyttjas som reservsystem i datakommunikationen och tidssynkroniseringen.
- Säkerställa de internationella leveranskedjorna för rymdtjänster och stärka de nationella aktörernas inhemska ägarskap.
- Vid lämpliga objekt ta i bruk de verifierade satellittjänster som EU:s rymdprogram erbjuder för myndigheter och kritisk infrastruktur.
- Uppföljning av cybersäkerheten som en del av lägesbilden av rymdläget i samarbete med olika aktörer
- Beakta cybersäkerheten i rymdsystemen i tillstånden, tillståndsvillkoren och hanteringen av systemens livscykel.

**Tidtabell och finansiering**

2025–2030 omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Tillgången till rymdtjänster och tjänsternas kontinuitet förbättras. Den kritiska infrastrukturen kan stödja sig på rymdtjänster och förbereda sig på störningar i dem.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**KM, ANM, IM,** SRK, FBC, Traficom

**Åtgärd 2.13**

**Informationssäkerheten hos enheter och program förbättras genom att säkerställa ett smidigt och effektivt genomförande av EU:s förordning om cyberresiliens (CRA)**

**Korg 1**

**Mål**

- Främja tillträde till marknaden och konkurrensen på EU:s inre marknad för tillverkare av utrustning och programvara som innehåller ett digitalt element.
- Säkerställa myndighetens förmåga att smidigt godkänna ett tillräckligt antal anmälda organ som gör en tredje parts bedömning och på så sätt förebygga flaskhalsar vid inträde på marknaden.
- Främja informationssäkerhetsnivån för apparater och program genom att ge företagen anvisningar om nya krav samt genom att ordna marknadskontrollen av dem på ett ändamålsenligt och smidigt sätt.
- Säkerställa Cybersäkerhetscentrets förmåga att koordinera anmälningar om sårbarheter hos apparater och program på det sätt som förutsätts i förordningen.
- Stödja den behöriga myndighetens uppgifter i cybersäkerhetscertifieringen när efterfrågan på certifieringar ökar till följd av verkställandet av förordningen om cyberresiliens.

**Tidtabell och finansiering**

2026–2030

Omkostnader, till en del tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Rättsakten om cyberresiliens är en central ny EU-förordning som ställer minimikrav på informationssäkerheten för apparater och program som kan kopplas till internet eller en annan enhet. Förordningen börjar tillämpas stegvis under 2026–2027. Ett lyckat verkställande av förordningen har stor betydelse för informationssäkerheten vid användning av utrustning och programvara samt för de finländska företagens konkurrenskraft, det vil säga utrustnings- och programtillverkarnas tillträde till EU-marknaden och konkurrensen på den inre marknaden. Genom förordningen säkerställs att produkterna är mindre sårbara och att tillverkarna ansvarar för cybersäkerheten under produktens hela livscykel.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**KM**, Traficom

## Pelare III: Samarbete
## ”En stabil nationell och internationell samarbetsmodell”

**Åtgärd 3.1**

**Samordningen av målen för den nationella cyberpolitiken utvecklas för att främja Finlands internationella profilering och genomslagskraft**

**Korg 1**

**Mål**

- Utveckla Finlands aktiva deltagande i centrala bilaterala och multilaterala nätverk och samarbete, och påverka aktivt i internationella organisationer, särskilt inom EU och Nato.
- Skapa en nationell samordningsmodell för internationellt samarbete inom cybersäkerhet och cyberförsvar.
- Genomföra aktivt strategiskt och operativt samarbete med nyckelländer.
- Påverka beaktandet av cybersäkerhetsaspekter i EU-reglering och internationella avtal.
- Sträva efter att främja internationell tillämpning av en samarbetsmodell som grundar sig på Finlands övergripande säkerhet och beredskap.

**Tidtabell och finansiering**
Från och med 2024
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Finland har uppnått sina kritiska mål i en internationell kontext.
Nödvändiga arrangemang och avtal har ingåtts och strategiskt och operativt samarbete har inletts.

EU-Nato-samarbetet stöder Finlands cybersäkerhet och cyberförsvar. En nationell lägesbilds- och samordningsmodell för den internationella cyberpolitiken har skapats och etablerats.

Finland har aktivt bidragit till utvecklingen av prioriteringarna och huvudfunktionerna i EU-Nato-samarbetet i en riktning som stöder den nationella cybersäkerheten och cyberförsvaret.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**UM, SRK, Cybersäkerhetsdirektören, FSM,** KM, Traficom, Försvarsmakten

**Åtgärd 3.2**

**Säkerheten i det internationella utbytet av hälsouppgifter utvecklas**

**Korg 1**

**Mål**

- European Health Data Space / Beredning av genomförandet av den primära och sekundära användningen av social- och hälsovårdsuppgifter och i genomförandefasen görs en riskbedömning.

**Tidtabell och finansiering**

2025–2031
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Cybersäkerhetsnivån säkerställs nationellt så att den motsvarar verksamhetsmiljön för EU:s informationsutbyte.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**SHM**, FPA, THL, Valvira

**Åtgärd 3.3**

**Åtgärderna i utredningen om myndigheternas verksamhetsförutsättningar inom cybersäkerheten förverkligas till den del de inte är en del av andra åtgärder**

**Korg 1**

**Mål**

- Förbättra samarbetet och processerna mellan myndigheterna och den privata sektorn samt informationsutbytet inom beredskapen och responsen, inklusive lagstiftningen.
- Identifiera aktörer som tillhandahåller vitala funktioner för samhället samt deras leveranskedjor.
- Uppdatera ordlistan för cybersäkerheten.
- Beakta cyberverksamhetsmiljön i beredskapslagstiftningen och genomföra lagstiftningsändringar som gör det möjligt att bistå kritiska företag.
- Utveckla gemensamma tekniska lösningar för informationsutbyte med hög säkerhetsklassificering.

**Tidtabell och finansiering**

2025–2030
Delvis tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Ett effektivt samarbete inom den offentliga förvaltningen möjliggörs genom avancerade lösningar för behandling av säkerhetsklassificerad information och information som kräver särskilt skydd.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**IM, FSM, UM, FM, KM,** Cybersäkerhetsdirektören, SRK, JM, Traficom, Försvarsmakten, Valtori, CKP, Skypo

**Åtgärd 3.4**

**Ansvaret i utvecklingen av det nationella cyberförsvaret förtydligas**

**Korg 1**

**Mål**

- I cyberförsvarsdoktrinen beskrivs verksamhetsmodellen för samarbete inom det nationella cyberförsvaret.
- Myndigheternas operativa samarbetsstruktur gör det möjligt att samordna myndigheternas operativa samarbete i cyberförsvarets uppgifter under alla förhållanden.
- Samarbetet, informationsutbytet och responsen utvecklas med beaktande av behoven mellan olika sektorer inklusive lagstiftningen: civil-militär samverkan, samarbete mellan myndigheter och den privata sektorn, samarbete inom försvars- och säkerhetssektorn, samarbete inom det frivilliga försvaret.

**Tidtabell och finansiering**

2025–2032
Tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Samarbetsstrukturerna på olika nivåer har bildats, verksamheten pågår och det finns en utvecklingsplan för den.

Samarbetet har utvecklats för att stödja situationsförståelsen inom cyberförsvaret och verkställandet av uppgifter (inklusive motåtgärder).

Cyberförsvaret kan på ett koordinerat sätt stödja andra myndigheter och sektorer med sina kunskaper och sin prestationsförmåga.

Finland framstår som en enhetlig aktör inom cyberförsvaret.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**FSM, Försvarsmakten**, övriga ministerier och myndigheter, FBC, näringslivet, organisationer

**Åtgärd 3.5**

**Säkerställa att aktuella anvisningar för cybersäkerhet är lättillgängliga för offentlig förvaltning, företag, medborgare och organisationer**

**Korg 2**

**Mål**

- Skapa och upprätthålla en nationell databank och tjänstekatalog för cybersäkerhetsanvisningar inklusive anvisningar för social- och hälsovården.
- Sammanställa och dela god praxis inom den offentliga förvaltningen för att genomföra cybersäkerheten så att den kan utnyttjas gemensamt via en gemensam kanal.

**Tidtabell och finansiering**

2024–2028
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Den gemensamma databanken för anvisningar effektiviserar åtgärderna för att förbättra cybersäkerheten och samarbetet i samhället.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**FM, SHM,** MDB

**Åtgärd 3.6**

**Produktionen och distributionen av lägesbilden av cybersäkerheten utvecklas och olika organisationers situationsmedvetenhet stärks**

**Korg 1**

**Mål**

- Utveckla produktionen av den strategiska lägesbilden så att den tillgodoser målgruppernas behov och se till att cybersäkerhetshändelser förmedlas till Statsrådets lägescentral.

- Säkerställa kontinuiteten i och tillgången till lägesbildsprodukter från Traficoms Cybersäkerhetscenter för rätt målgrupper.
- Utveckla samarbetsnätverkens verksamhet så att den motsvarar den förändrade verksamhetsmiljön och trygga nätverkens verksamhet.
- Utveckla samarbetet mellan tillsynsmyndigheterna (NIS2) och dataombudsmannen samt den gemensamma hanteringen av incidenter.

**Tidtabell och finansiering**

2025–2027
Tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Genom att granska målgrupperna för lägesbilden säkerställs tillgången till lägesbildsinformation i rätt tid i stor utsträckning i samhället.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**KM, SRK,** Traficom, dataombudsmannen, övrig offentlig förvaltning

**Åtgärd 3.7**

**Den offentliga sektorn utvecklar och tillhandahåller centraliserade cybersäkerhetstjänster tillsammans med den privata sektorn**

**Korg 1**

**Mål**

- Kontinuiteten i de tjänster som Traficoms Cybersäkerhetscenter producerar säkerställs och användningen av tjänsterna, såsom Cybermätaren och Hyöky, utvidgas till större målgrupper.
- Effektiviteten hos MDB:s Vahti-nätverk, Taisto-övningar och Julkri-verktyg stärks.
- Öka användningsgraden, effektiviteten och utnyttjandet av MDB:s administrativa helhetsbild för den digitala säkerheten inom den offentliga förvaltningen.
- Producera mallar, förhandla centraliserat om avtal.
- Identifiera och utveckla nya tjänster som behövs.

**Tidtabell och finansiering**

2024–2030
Omkostnader, till en del tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Gemensamma centraliserade cybersäkerhetstjänster effektiviserar resursanvändningen. En omfattande användning av dem är en förutsättning för en betydande förbättring av de offentliga tjänsternas säkerhet och funktionssäkerhet. Tryggande av tjänsternas kontinuitet, nya tjänster och en utvidgning av tjänsterna förutsätter tilläggsresurser.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**KM, FM**, FBC, Traficom, MDB, ICT-bolag inom den offentliga förvaltningen, den privata sektorn, övrig offentlig förvaltning

**Åtgärd 3.8**

**Säkerheten och funktionssäkerheten hos gemensamma informations- och kommunikationstekniska tjänster och datalager främjas**

**Korg 1**

**Mål**

- Genomföra programmet för utveckling av säkerheten hos gemensamma informations- och kommunikationstekniska tjänster (PATO).
- Skydda kritiska datalager och geografisk information om kritiska objekt.
- Säkerställa det operativa informationsutbytet och ledningen genom en gemensam säker lösning för informationsutbyte för att garantera kritisk kommunikation.

**Tidtabell och finansiering**

2024–2030
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

De gemensamma funktionssäkra informations- och kommunikationstekniska tjänsterna stöder störningsfri samhällsverksamhet och möjliggör ett effektivt genomförande av de strategiska uppgifterna.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**FM,** Valtori, ERVE

**Åtgärd 3.9**

**Bestämmelserna om säkerhetsnätet och gemensamma informations- och kommunikationstekniska tjänster förnyas**

**Korg 2**

**Mål**

- Möjliggöra utnyttjande av myndigheternas cyberförmågor för att skydda produktionen av statsförvaltningens gemensamma informations- och kommunikationstekniska tjänster genom bestämmelser och avtal.

**Tidtabell och finansiering**

2026–2029
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Myndigheternas resurser används så effektivt som möjligt för att trygga produktionen av gemensamma informations- och kommunikationstekniska tjänster och de strategiska uppgifterna enligt säkerhetsstrategin för samhället.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**FM,** FSM, Försvarsmakten, Valtori

**Åtgärd 3.10**

**Behovet av att utveckla bestämmelserna om säkerhetsklassificering utreds**

**Korg 1**

**Mål**

- Utreda säkerhetsklassificeringsbestämmelsernas tillämplighet med beaktande av molntjänster och artificiell intelligens samt genomföra nödvändiga författningsändringar.
- Utreda tillämpningsområdet för skyldigheten till säkerhetsklassificering och förtydliga anvisningarna i synnerhet i välfärdsområdena, kommunerna och bolagen med specialuppgifter samt vid behov genomföra författningsändringar.
- I samband med eventuella författningsändringar granskas förenligheten med internationella författningar.

**Tidtabell och finansiering**

2025–2029
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Uppdaterade säkerhetsklassificeringsbestämmelser och ett ändamålsenligt tillämpningsområde och anvisningar för klassificeringsskyldigheten förbättrar den nationella cybersäkerheten.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**FM, UM**

## Pelare IV: Reaktion och motåtgärder
## ”Reagerande på hot i rätt tid och tryggad suveränitet”

### Åtgärd 4.1

**Välfärdsområdenas beredskap och förmåga att förbereda sig och reagera i rätt tid på cyberstörningar utvecklas**

**Korg 2**

**Mål**

- Välfärdsområdena har klassificerat sina centrala informationssystem och funktioner enligt en enhetlig klassificering av kritiskhet.
- Förtydliga förfarandena för anmälan av avvikelser i välfärdsområdena.
- Stärka samarbetsnätverket mellan beredskapscentren för social- och hälsovården (5) och de nationella aktörerna och införa en ny riskhanteringsmodell för välfärdsområdena för att utveckla hanteringen av ICT-störningar.
- Garantera säkerheten i social- och hälsovårdens nationella tjänster.

**Tidtabell och finansiering**

2024–2030
Omkostnader, till en del tilläggsresurser
Utvecklingen sker också som en del av FBC:s program DT2030.

**Konsekvensbedömning och effektivitetsanalys**

Välfärdsområdenas förmåga att förbereda sig och reagera på cyberhot i verksamhetsmiljön förbättras.
Man upprätthåller medvetenheten om cybersäkerheten som en del av utvecklingen av social- och hälsovårdsorganisationernas verksamhet.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**SHM, JM,** FM, IM, välfärdsområdena, Traficom, Valvira, dataombudsmannen, näringslivet

**Åtgärd 4.2**

**Kommunernas beredskap och förmåga att förbereda sig och reagera i rätt tid på cyberstörningar utvecklas**

**Korg 2**

**Mål**

- Stärka riskhanteringen, den kontinuerliga förbättringen, säkerhetskulturen och spridningen av bästa praxis inklusive VIRT-verksamheten (Virtual Incident Response Team), ICT-beredskapen, störningshanteringen, säkra upphandlingar och molntjänsternas säkerhet i lämpliga nationella, regionala och lokala nätverk mellan kommunerna.
- Upprätthålla och utveckla väsentliga nationella informationssäkerhets- och dataskyddsnätverk för att möjliggöra nätverkande och delning av information mellan organisationer.
- Kommunerna genomför en klassificering av kritiskhet av centrala informationssystem och funktioner.

**Tidtabell och finansiering**

2024–2030
Omkostnader
Utvecklingen sker också som en del av FBC:s program DT2030.

**Konsekvensbedömning och effektivitetsanalys**

Kommunernas förmåga att förbereda sig och reagera på cyberhot i verksamhetsmiljön förbättras.

Effektivitet: nationell/betydande.

**Ansvarar**/aktörer

**FM,** kommunerna, MDB, Traficom, övrig offentlig förvaltning, näringslivet

**Åtgärd 4.3**

**Stärka de kritiska branschernas beredskap och reaktioner på cyberavvikelser**

**Korg 2**

**Mål**

- Stödja beredskapen för kritiska branscher och svar på cyberstörningar och personuppgiftsincidenter bland annat genom att utnyttja EU:s mekanism för cybersäkerhet i nödsituationer.
- Främja att finländska leverantörer av informationssäkerhetstjänster deltar i EU:s cybersäkerhetsreserv.
- Utnyttja EU:s cybersäkerhetsreserv för att svara på betydande eller omfattande avvikelser.
- Förbättra dataombudsmannens verksamhetsförutsättningar.

**Tidtabell och finansiering**

Från och med 2025
Delvis tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Möjliggör eller påskyndar genomförandet av åtgärder som förbättrar cybersäkerheten i organisationerna och förbättrar därigenom organisationernas beredskap och förmåga att förbereda sig och reagera i rätt tid på cybersäkerhetsstörningar.

I EU-finansierade beredskapsåtgärder krävs nationell medfinansiering motsvarande 50 procent.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**KM, JM,** Traficom, dataombudsmannen

**Åtgärd 4.4**

**Trygga den nationella observationsförmågan (HAVARO)**

**Korg 1**

**Mål**

- Trygga HAVARO-tjänstens funktion och kontinuitet. (HAVARO = nationellt system som upptäcker och varnar för allvarliga kränkningar av dataskyddet).
- Främja utnyttjandet av HAVARO för att trygga samhällets vitala funktioner.

**Tidtabell och finansiering**

2026–2030
Tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

HAVARO-tjänsten producerar information med hjälp av vilken de organisationer som använder tjänsten bygger upp och utvecklar sitt eget cyberskydd.

Genom att trygga HAVARO:s kontinuitet säkerställs den nationella observationsförmågan och den nationella cybersäkerheten upprätthålls.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**KM**, Traficom, FBC

**Åtgärd 4.5**

**Det säkerställs att underrättelsemyndigheterna har tillräcklig förmåga att inhämta information**

**Korg 2**

**Mål**

- Utveckla förmågan att observera statligt cyberspionage och påverkan och säkerställa resurser för det.
- Utveckla cyberunderrättelsen så att den motsvarar förändringarna i verksamhetsmiljön.

**Tidtabell och finansiering**

2025–2035
Tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Observationerna av cyberspionage har en central betydelse för att identifiera hot och begränsa konsekvenserna.

Effektivitet: nationell och internationell/stor.

**Ansvarar**/aktörer

**IM, FSM,** Försvarsmakten, Skypo

**Åtgärd 4.6**

**Utveckla myndigheternas samarbete, lägesbild och observation av hot och stärka deltagandet i det internationella samarbetet**

**Korg 2**

**Mål**

- Stärka det nationella myndighetssamarbetet, lägesbilden och observationsförmågan genom att utnyttja finansieringsmöjligheterna i EU:s larmsystem för cybersäkerhet.
- Stärka det internationella samarbetet genom att delta i gränsöverskridande lägesbildssamarbete enligt cybersolidaritetsakten.
- Skapa en nationell cybersäkerhetskoncentration vid Traficoms Cybersäkerhetscenter som deltar i gränsöverskridande samarbete och effektiviserar den nationella lägesbilden och spridningen av hotinformation.

**Tidtabell och finansiering**

2025–2032
Delvis tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Genom att effektivt observera hot och dela lägesbilden kan man förebygga cyberstörningar och minska effekterna av dem.

Genom att delta i gemensamma upphandlingar av lägesbilds- och observationsförmåga på EU-nivå kan man uppnå besparingar, effektivisera insamlingen av lägesbilden och påskynda observationen av hot tillsammans med EU-medlemsländerna.

Effektivitet: nationell och internationell/stor.

**Ansvarar**/aktörer

**KM, SRK, FSM, IM,** Traficom, Försvarsmakten, övriga säkerhetsmyndigheter

**Åtgärd 4.7**

**Trygga resurser för bekämpning av allvarlig och organiserad IT-brottslighet och nätbaserad brottslighet samt cyberförsvar**

**Korg 1**

**Mål**

- Säkerställa och utveckla brottsbekämpningens och brottsutredningens förmåga samt förverkligande av straffansvaret.
- Samarbetet mellan brottsbekämpningen och cyberförsvaret utvecklas särskilt i fall som gäller statlig verksamhet.

**Tidtabell och finansiering**

Från och med 2024
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Med tanke på förverkligande av straffansvaret och ett fungerande samhälle är det viktigt att polisen har tillräcklig förmåga att undersöka fall av allvarlig och organiserad IT-relaterad brottslighet samt erbjuda stöd till brottsbekämpande myndigheter i andra länder.

Motsvarande förmåga behövs för att genomföra Försvarsmaktens uppgifter inom cyberförsvaret och i den omfattning som fastställs i lagen om militär disciplin och brottsbekämpning inom försvarsmakten.

Effektivitet: nationell och internationell/mycket stor

**Ansvarar**/aktörer

**IM,** FSM, Polisstyrelsen

**Åtgärd 4.8**

**Det internationella brottsbekämpningssamarbetet för att bekämpa IT-brott (J-CAT) etableras**

**Korg 2**

**Mål**

- Etablera internationell operativ verksamhet för bekämpning av cyberbrott. Säkerställa operativt samarbete som möjliggör bekämpning av internationell allvarlig och organiserad brottslighet.

**Tidtabell och finansiering**

Från och med 2024
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Den allvarliga cyberbrottsligheten är definitionsmässigt internationell och J-CAT-samarbetet har visat att internationellt operativt arbete är nödvändigt, och J-CAT erbjuder en fungerande plattform för detta.

Effektivitet: nationell och internationell/stor.

**Ansvarar**/aktörer

**IM**, Polisstyrelsen, CKP

**Åtgärd 4.9**

**Samarbetet mellan myndigheterna intensifieras för att förbättra och förebygga lägesbilden för nätbaserad brottslighet**

**Korg 2**

**Mål**

- Utreda de vanligaste sätten att begå brott, hur vanliga de är och god praxis för att förebygga dem samt de brottsskador som dessa orsakar.
- Utifrån lägesbilden påverka identifierade hot och aktörer.
- Upplysa medborgarna med hjälp av god praxis.
- Utveckla samarbetet mellan flera myndigheter för bekämpning av näthandelsbedrägerier och samarbetet med webbutiksaktörer (näringslivet).

**Tidtabell och finansiering**

Från och med 2025
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Lägesbilden för nätbaserad brottslighet förbättras och utifrån den påverkas förebyggandet av de vanligaste tillvägagångssätten.

Effektivitet: nationell/stor.

**Ansvarar**/aktörer

**JM, IM, ANM,** Rådet för brottsförebyggande, Polisen, Traficom, KKV, konsumentombudsmannen, dataombudsmannen

**Åtgärd 4.10**

**En nationell attributram bereds**

**Korg 1**

**Mål**

- Skapa en nationell attributram.
- Förtydliga processerna, myndighetsrollerna och myndigheternas ansvar (tekniskt, operativt och politiskt).

**Tidtabell och finansiering**

Från och med 2024
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Attributramen stöder effekterna av Finlands utrikes- och säkerhetspolitik bland annat genom att utveckla beredskapen att reagera på fientlig cyberverksamhet samt genom att främja regelbaserad verksamhet och ansvarsfullt statligt beteende i cyberverksamhetsmiljön.
Attributramen utvecklar förmågan och beredskapen att attribuera cyberhot som riktas mot Finland samt ger stöd till internationella organisationer och partner.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**UM**, SRK, IM, FSM, KM, Cybersäkerhetsdirektören, Republikens presidents kansli, underrättelsemyndigheterna, Traficom, Försvarsmakten, CKP

**Åtgärd 4.11**

**Cyberförsvarsdoktrin utarbetas**

**Korg 1**

**Mål**

- Upprätta och godkänna en doktrin.
- Identifiera och förtydliga processerna, myndighetsrollerna och myndigheternas ansvar inom cyberförsvaret.
- Beskriva principerna för övervakning, skydd och tryggande av den statliga suveräniteten.
- Uppdatera Finlands principbeslut om tillämpning av internationell lagstiftning.
- Utveckla grunderna för utvärderingen av effekterna av cybermotåtgärder och cyberoperationer på såväl strategisk som operativ nivå.

**Tidtabell och finansiering**

2024–2026
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Cyberförsvarsdoktrinen skapar förmåga till övergripande och samordnad respons och motåtgärder mot fientlig verksamhet.

Samarbetet och målmedvetenheten utvecklas.

Förmågan att stödja de allierade och utnyttja deras förmågor i det nationella cyberförsvaret utvecklas.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**FSM, UM**, SRK, IM, KM, Republikens presidents kansli, Försvarsmakten, Cybersäkerhetsdirektören, Traficom, Skypo, Polisen

**Åtgärd 4.12**

**Det nationella och militära cyberförsvaret utvecklas och deras integration med Nato slutförs**

**Korg 1**

**Mål**

- Uppdatera författningsgrunden för cyberförsvarets uppgifter och befogenheter.
- Uppdatera författningsgrunden för tryggandet av den statliga suveräniteten.
- Fortsätta utvecklingen av cyberförsvarets prestationsförmåga på nationell, operativ och lokal nivå.
- Möjliggöra flexibel handräckning och liknande hjälp mellan olika myndigheter.
- Integrationen av totalförsvaret och försvarssystemet är klar i fråga om cybersäkerheten.
- Det nationella resiliensarbetet har genomförts, förts in i beredskapsplanerna och övats.

**Tidtabell och finansiering**

2024–2032
Delvis tilläggsresurser

**Konsekvensbedömning och effektivitetsanalys**

Den statliga suveräniteten tryggas.

Man skapar förmåga till nationell övergripande och samordnad respons och motåtgärder.

Finland kan fungera som en del av alliansen och dess avskräckande effekt och försvar även i cybermiljön.

Finland kan ge och ta emot hjälp.

Finland kan stödja allierade som är verksamma i området även i en bestridd cybermiljö.

Effektivitet: nationell och internationell/mycket stor.

**Ansvarar**/aktörer

**FSM, Försvarsmakten,** UM, KM, IM, övriga ministerier, övriga myndigheter och aktörer på lokal och regional nivå, det kritiska företagsfältet

**Åtgärden**

**Finland producerar uppgifter för enkäter om internationella cybersäkerhetsindex (Cybersäkerhetsindex från Internationella teleunionen ITU (Global Cyber Index, GCI) och nationellt cybersäkerhetsindex (e-Governance Academys National Cyber Security Index, NCSI)**

**Mål**

- Finland placerar sig bland de ledande länderna i mätningar med internationella index.

**Tidtabell och finansiering**

Från och med 2026
Omkostnader

**Konsekvensbedömning och effektivitetsanalys**

Indikatorerna utnyttjas som stöd för det nationella utvecklingsarbetet.

Effektivitet: nationell/mycket stor.

**Ansvarar**/aktörer

**Cybersäkerhetsdirektören**, uppföljningsgruppen för strategin