Bilaga 1: Handlingsplan 2026

Nationell strategi för cybersäkerhet 2025–2029

Regeringskansliet
Försvarsdepartementet

Handlingsplan

Regeringen antog en nationell strategi för cybersäkerhet 2025–2029 den 20 mars 2025. Till strategins pelare och mål kopplas denna handlingsplan, som innehåller ett antal aktiviteter som svarar mot regeringens inriktning. Handlingsplanen omsätter strategin i konkret handling genom aktiviteter i form av bland annat specifika uppdrag och styrning av myndigheter. Utvärdering och revidering av handlingsplanens innehåll sker i den omfattning regeringen bedömer som nödvändig, och innehållet uppdateras löpande för att stegvis bidra till att målen uppnås.

I denna uppdaterade version har ett antal aktiviteter justerats, tillkommit, genomförts eller avslutats. För att tydliggöra vilka förändringar som har gjorts markeras de aktiviteter vars innehåll i sak har ändrats med beteckningen ”Uppdaterad”. Med ändring i sak avses exempelvis att aktivitetens innebörd har justerats eller att tidsperioden har ändrats. Redaktionella ändringar, förtydliganden eller organisatoriska anpassningar som inte påverkar aktivitetens innebörd i sak medför inte att aktiviteten markeras som uppdaterad.

Den 1 januari bytte Myndigheten för samhällsskydd och beredskap (MSB) namn till Myndigheten för civilt försvar (MCF). Vidare kommer MCF:s uppgifter på cybersäkerhetsområdet att föras över till det nationella cybersäkerhetscentret (NCSC) vid Försvarets radioanstalt (FRA) den 1 juli 2026. Sådana organisatoriska förändringar medför inte att berörda aktiviteter markeras som uppdaterade.

Aktiviteter som har slutförts markeras som ”Genomförd” och aktiviteter som inte längre är aktuella eller bedöms sakna behov av fortsatt genomförande markeras som ”Avslutad”. Sådana aktiviteter behåller sina ursprungliga namn och löpnummer för att säkerställa spårbarhet över tid. Nya aktiviteter markeras som ”Ny” och tilldelas ett nytt löpnummer inom det mål som de hör till.

Totalt innehåller den uppdaterade handlingsplanen 91 aktiviteter jämfört med 72 aktiviteter i den ursprungliga handlingsplanen från 2025. 21 nya aktiviteter har tillkommit och 2 aktiveter har genomförts eller avslutats. 13 aktiviteter har uppdaterats.

betyder ansvarig utförare för aktiviteten.

betyder tidsperiod för åtgärdens genomförande.

Pelare A: Systematiskt och effektivt cybersäkerhetsarbete

Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer

1.1 Nationellt cybersäkerhetscenters (NCSC) verksamhet inom Försvarets radioanstalt (FRA) bedrivs utifrån en ny förordning.

Syfte: Att ge tydlig och långsiktig styrning som lägger grunden för ett välfungerande NCSC och tydliggör dess roll i det nationella cybersäkerhetsarbetet.

Regeringen

Tills vidare

1.2 **Uppdaterad:** CER-direktivet genomförs nationellt på ett harmoniserat sätt.

Syfte: Genom att CER-direktivet genomförs i svensk rätt på ett sätt som, när det är lämpligt, harmoniserar med cybersäkerhetslagen och cybersäkerhetsförordningen.

Regeringen

2026

1.3 **Uppdaterad:** Remittering och beredning av förslagen i betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning.

Fi 2024:07

2026

1.4 **Uppdaterad:** Myndigheten för civilt försvar (MCF) säkerställer att ett utbildningsutbud finns tillgängligt för organisationer som omfattas av NIS 2-direktivet och beredskapssektorerna.

Syfte: Aktiviteten stödjer målet genom att höja kompetensen hos organisationer som ska bedriva ett systematiskt cybersäkerhetsarbete.

MCF

2024–2027

1.5 NCSC vid FRA och MCF ska inom ramen för NCSC ta fram riktlinjer för att främja utveckling och integrering av relevant avancerad teknik som syftar till att genomföra moderna riskhanteringsåtgärder för cybersäkerhet i enlighet med artikel 7.2 i NIS 2-direktivet.

Syfte: Aktiviteten stödjer målet genom att främja moderna cyberriskhanteringsåtgärder som en del i organisationers cybersäkerhetsarbete.

NCSC vid FRA och MCF med bistånd av Försvarets materielverk (FMV), Försvarsmakten, Polismyndigheten, Post- och telestyrelsen (PTS) och Säkerhetspolisen

2025–2026

1.6 MCF fortsätter utveckla och förvalta råd och stöd för organisationers systematiska cybersäkerhetsarbete.

Syfte: Aktiviteten stödjer målet genom att organisationer kan få vägledning i sitt cybersäkerhetsarbete.

MCF

Tills vidare

1.7 MCF fortsätter arbetet med analyser och temarapporter inom cybersäkerhetsområdet.

Syfte: Myndighetens arbete med analyser och temarapporter är till gagn för organisationers cybersäkerhetsarbete och arbetet med att stärka samhällets motståndskraft.

MCF

Tills vidare

1.8 Finansinspektionen fortsätter utöva tillsyn över den finansiella sektorns cybersäkerhetsarbete och digitala operativa motståndskraft.

Syfte: Genom tillsyn säkerställer Finansinspektionen att den finansiella sektorn (som består i huvudsak av privata aktörer som tillhandahåller tjänster som bland annat betalningsförmedling och kapitalförvaltning) upprätthåller en hög nivå av cybersäkerhetsarbete och digital motståndskraft i enlighet med DORA-förordningens krav.

Finansinspektionen

Tills vidare

1.9 MCF vidareutvecklar Cybersäkerhetskollen för att kunna bistå fler organisationer i fler processer och kunna förmedla en fördjupad nationell lägesbild kring cybersäkerhetsnivån i samhällsviktiga verksamheter.

Syfte: Genom att utöka Cybersäkerhetskollen med stöd för bedömning av organisationens it- och operativ teknik-säkerhet samt leveranskedjor får organisationer ett ändamålsenligt verktyg att både bedöma sin nivå inom flera centrala områden och förslag på åtgärder för att hantera identifierade brister. Utvecklingen ger även tillgång till en bredare och mer fördjupad lägesbild som stöd för riktade insatser på nationell nivå.

MCF

2025–2027

1.10 **Ny:** Vetenskapsrådet ska ta fram och fastställa riktlinjer i syfte att ge stöd till lärosäten, forskningsinstitut och forskningsfinansiärer för att utveckla, förbättra och främja användningen av cybersäkerhetsverktyg och säker nätinfrastruktur i enlighet med artikel 7.2 i NIS 2-direktivet.

Syfte: Aktiviteten stödjer målet genom att lärosäten, forskningsinstitut och forskningsfinansiärer kan få stöd i sitt cybersäkerhetsarbete.

Vetenskapsrådet

2026

1.11 **Ny:** Naturvårdsverket tillförs medel.

Syfte: Förstärkt skydd mot cyberhot med anledning av det försämrade omvärldsläget.

Naturvårdsverket

2026

1.12 **Ny:** Energimyndigheten tillförs medel.

Syfte: Utvecklingsarbete i enlighet med det nya EU- regelverket inom cybersäkerhet för att säkerställa ett effektivt och rättssäkert arbete för en hög cybersäkerhetsnivå inom energisektorn.

Energimyndigheten

Tills vidare

1.13 **Ny:** Överföring av uppgifter på cybersäkerhetsområdet från MCF till NCSC vid FRA.

Syfte: En överföring av uppgifter på cybersäkerhetsområdet från MCF till NCSC ger goda förutsättningar för ett mer sammanhållet och fokuserat arbete där NCSC utgör navet i Sveriges cybersäkerhetsarbete.

MCF och NCSC vid FRA

2026

1.14 **Ny:** NCSC vid FRA tillförs medel.

Syfte: NCSC ska utgöra navet i det nationella cybersäkerhetsarbetet och har en väsentlig roll inom flertalet av målområdena i cybersäkerhetsstrategin. För att kunna höja cybersäkerhetsförmågan avser regeringen öka tilldelningen av medel till NCSC, framför allt personella resurser.

Regeringen

Tills vidare

1.15 **Ny:** NCSC vid FRA ska genomföra mätning av resultatindikatorer.

Syfte: Aktiviteten stödjer målet genom att NCSC ska ta fram mätmetoder för och genomföra mätning av de resultatindikatorer som anges i Nationell strategi för cybersäkerhet 2025–2029 (skr. 2024/25:121).

NCSC vid FRA

2026

Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering

2.1 MCF ska med stöd av FRA och FMV genomföra en nationell kartläggning av kommuners tekniska cybersäkerhetsförmåga. Kartläggningen ska ske genom upphandlade it-säkerhetsanalyser utförda av privata företag.

Syfte: Kartläggningen ska identifiera åtgärder som kommuner själva kan vidta kostnadseffektivt, och också vara stöd i att göra prioriteringar av nödvändiga framtida investeringar inom cybersäkerhetsområdet. Kartläggningen ska samlat ge underlag för förbättrad kravställning av it-säkerhetsåtgärder, och för att kunna göra prioriteringar av nödvändiga framtida investeringar inom cybersäkerhetsområdet på nationell nivå.

MCF med stöd av FRA och FMV

2025–2027

2.2 Över 100 myndigheter implementerar uppdrag att redogöra för hur de förvaltat och utvecklat sitt arbete med informations- och cybersäkerhet.

Syfte: Att skärpa myndigheternas återrapporteringskrav och prioriterar arbetet inom informations- och cybersäkerhet och ger regeringen underlag för ytterligare åtgärder på området.

Berörda statliga myndigheter

2025–2026

2.3 MCF etablerar en kompletterande analysmiljö till Cybersäkerhetskollen där drift, förvaltning och utveckling ingår.

Syfte: Aktiviteten stödjer målet genom utveckling av verktyget och därmed ökade förutsättningar för samhällsviktiga verksamheter att nyttja det för att nå en tillfredställande cybersäkerhetsnivå.

MCF

2025–2027

2.4 **Uppdaterad:** NCSC vid FRA och MCF ska ta fram riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för produkter inom informations- och kommunikationsteknik (IKT), IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod i enlighet med artikel 7.2 i NIS 2-direktivet.

Syfte: Att erbjuda vägledning avseende säkrare upphandling vilket är av särskild vikt för att höja cybersäkerheten i statlig och kommunal förvaltning.

NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

2.5 **Uppdaterad:** Regeringskansliet uppdaterar strategins bilaga 2, ”Organisationer med roller och ansvarsområden inom cybersäkerhet”, när organisationsförändringar och ansvarsfördelning trätt i kraft i enlighet med aktivitet 1:13 i denna handlingsplan.

Syfte: Aktiviteten stödjer målet genom att Regeringskansliet klargör hur ansvaret för det nationella cybersäkerhetsarbetet är fördelat.

Regeringskansliet

2026

2.6 **Genomförd:** Uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet.

Syfte: Att stärka den nationella cybersäkerheten och motståndskraften genom en samlad och samordnad styrning av samhällets informations- och cybersäkerhetsarbete och en ändamålsenlig myndighetsstruktur.

Fö 2024:04

2024–2025

2.7 **Ny:** Försäkringskassan, Lantmäteriet, Skatteverket och Trafikverket erbjuder it-driftstjänster inom ett samordnat statligt tjänsteutbud och tillhandahåller dessa till intresserade myndigheter.

Syfte: Aktiviteten stärker statens cybersäkerhet och ökar robusthet, motståndskraft och kostnadseffektivitet genom en enhetlig, kvalitetssäkrad och säker struktur för statlig it-drift.

Försäkringskassan, Skatteverket, Trafikverket, Lantmäteriet

Tills vidare

Mål 3: Stärkt säkerhetsarbete inom kritisk infrastruktur

3.1 MCF tillhandahåller stöd för samhällsviktig verksamhets arbete med säkerhet i operativ teknik (OT).

Syfte: Aktiviteten stödjer målet genom att inom ramen för befintliga stödtjänster såsom metodstödet och Cybersäkerhetsrådgivningen erbjuda operatörer stöd kring säkerhet i de OT-system som kritisk infrastruktur ofta är beroende av.

MCF

Tills vidare

3.2 NCSC vid FRA och MCF ska ta fram riktlinjer för att upprätthålla den allmänna tillgängligheten, integriteten och konfidentialiteten hos den offentliga kärnan i det öppna internet. Inbegripet, i tillämpliga fall, cybersäkerheten hos undervattenskablar i enlighet med artikel 7.2 i NIS 2-direktivet.

Syfte: Aktiviteten stödjer målet genom anpassade riktlinjer avseende säker och tillgänglig konnektivitet, vilket samhället är beroende av.

FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

3.3 Hotbildsstyrda penetrationstester genomförs regelbundet på organisationer inom den finansiella sektorn.

Syfte: Hotbildsstyrda penetrationstester syftar till att en aktör inom den finansiella sektorn ska kunna bedöma sin beredskap att hantera it-incidenter, identifiera svagheter, brister och luckor i den digitala motståndskraften och snabbt genomföra korrigerande åtgärder. Enligt DORA-förordningen ska finansiella entiteter som har central betydelse för det finansiella systemet regelbundet genomföra sådana tester. Finansinspektionen beslutar om vilka entiteter som ska göra dessa tester och Riksbanken ska övervaka och samordna testerna.

Finansinspektionen och Sveriges Riksbank

Tills vidare

Mål 4: Robustare digitala leveranskedjor och minskat beroende

4.1 Berörda statliga myndigheter fortsätter bidra till standardisering av cybersäkerhet inom ramen för NCSC-samverkan.

Syfte: Att genom myndighetsgemensam samordning samverka frågor av myndighetsöverskridande relevans kring internationell standardisering på cybersäkerhetsområdet.

PTS och FMV i samverkan med Försvarsmakten, FRA, MCF Säkerhetspolisen och Polismyndigheten

Tills vidare

4.2 FMV deltar i samarbeten och aktiviteter som bedrivs inom ramen för EU:s ramverk för cybersäkerhetscertifiering. I dessa sammanhang ska myndigheten bland annat söka få genomslag för svenska ståndpunkter och verka för att nya certifieringsordningar tas fram på ett transparent sätt.

Syfte: Aktiviteten stödjer målet genom att transparenta och välanpassade certifieringsordningar kan användas för att höja cybersäkerhetsnivån för it-produkter, it-tjänster, it-processer och utlokaliserade säkerhetstjänster.

FMV

Tills vidare

4.3 MCF genomför en kartläggning av digitala leveranskedjor och tar fram en modell för uppföljning av digitala leveranskedjor.

Syfte: Att kartlägga digitala leveranskedjor inom vissa sektorer och identifiera särskilt skyddsvärda digitala leveranskedjor samt bedöma förekomsten av monoberoenden och kritiska beroenden till tredjeland. Därtill syftar uppdraget till att möjliggöra framtagandet av en modell för uppföljning av digitala leveranskedjor som kompletterar den befintliga struktur för uppföljning av det systematiska informationssäkerhetsarbetet i den offentliga förvaltningen som regeringen den 19 september 2019 uppdrog MSB att upprätta (Ju2019/03058/SSK och Ju2019/02421/SSK).

MCF

2025–2026

4.4 NCSC vid FRA och MCF ska ta fram riktlinjer för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter när de tillhandahåller sina tjänster, i enlighet med artikel 7.2 i NIS 2-direktivet.

Syfte: Aktiviteten stödjer målet genom att bidra till organisationers möjlighet att säkra sina leveranskedjor och därmed minska sin sårbarhet för cyberangrepp och störningar.

NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

Mål 5: Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete

5.1 **Uppdaterad:** MCF är nationell gemensam kontaktpunkt i enlighet med NIS 2-direktivet.

Syfte: Aktiviteten stödjer målet genom att MCF i egenskap av kontaktpunkt bland annat bedriver tillsynssamordning via ett samarbetsforum för effektiv och likvärdig tillsyn kopplat till NIS 2-regleringen samt deltar i internationell samverkan rörande regulatoriska policyfrågor (Sveriges representant i NIS Cooperation Group).

MCF

2025

5.2 Berörda statliga myndigheter fortsätter inom ramen för NCSC arbetet med en nationell modell där föreskrifter, allmänna råd och vägledningar så långt som möjligt ensas så att de följer en likartad logik, struktur och terminologi.

Syfte: Aktiviteten stödjer målet genom att se över hur en samordnad regelutformning kan främja enklare regelefterlevnad, exempelvis genom myndighetsgemensam vägledning rörande it-säkerhetslösningar.

NCSC vid FRA, Försvarsmakten, MCF, Säkerhetspolisen och FMV

Tills vidare

5.3 Medel tillförs ett antal statliga myndigheter för att förbereda och utveckla sin tillsynsverksamhet utifrån NIS 2-direktivet.

Syfte: Aktiviteten stödjer målet genom att skapa bättre förutsättningar för tillsynsmyndigheter att hantera de ökade kraven rörande tillsyn som följer av cybersäkerhetslagen (2025:1506) och cybersäkerhetsförordningen (2025:1507).

Vissa länsstyrelser, Läkemedelsverket, Inspektionen för vård och omsorg, Transportstyrelsen, Livsmedelsverket, Statens energimyndighet och PTS

Tills vidare

5.4 Säkerhetspolisen och Försvarsmakten utvecklar löpande tillsynsverksamheten kring, och samarbetet mellan, myndigheter som har ansvar enligt säkerhetsskyddslagstiftningen.

Syfte: Aktiviteten stödjer målet genom att ändamålsenlig tillsyn kan bidra till bland annat cybersäkerheten i samhället.

Säkerhetspolisen och Försvarsmakten

Tills vidare

5.5 Säkerhetspolisen och Försvarsmakten utvecklar kontinuerligt stödjande material såsom vägledningar, handböcker och utbildningsmaterial inom säkerhetsskydd.

Syfte: Aktiviteten bidrar till att förenkla regelefterlevnaden för aktörer som träffas av cybersäkerhetskrav inom ramen för bland annat säkerhetsskyddsregleringen.

Säkerhetspolisen och Försvarsmakten

Tills vidare

5.6 MCF förvaltar, utvecklar och tillhandahåller en publik databas över svensk terminologi inom cybersäkerhetsområdet.

Syfte: Att säkerställa en ensad terminologi som förenklar organisationers cybersäkerhetsarbete och samarbete sinsemellan.

MCF

Tills vidare

5.7 MCF tillhandahåller och vidareutvecklar rådgivningstjänst med särskilt fokus på NIS 2-aktörer.

Syfte: Genom aktiviteten erbjuds verksamhetsutövare rådgivning som stöd för organisationers anpassning till att efterleva NIS 2-direktivets krav.

MCF

2025–2027

5.8 **Ny:** Regioner tillförs medel för ökad cybersäkerhet.

Syfte: Genom aktiviteten erbjuds verksamhetsutövare rådgivning som stöd för organisationers anpassning till att efterleva NIS 2-direktivets krav.

Regioner

Tills vidare

5.9 **Ny:** Kommuner tillförs medel för ökad cybersäkerhet.

Syfte: Att öka den offentliga förvaltningens motståndskraft mot cybersäkerhetsincidenter och cyberhot och för genomförande av det så kallade NIS 2-direktivet.

Kommuner

Tills vidare

5.10 **Ny:** Svenska lärosäten tilldelas medel för ökad cybersäkerhet och för implementering av cybersäkerhetslagen.

Syfte: Aktiviteten stödjer målet genom att svenska lärosäten får ökade förutsättningar att vidta åtgärder för att skydda sina nätverks- och informationssystem samt rapportera betydande incidenter.

Lärosäten

Tills vidare

Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete

6.1 NCSC vid FRA och MCF ska inom ramen för NCSC ta fram riktlinjer som stärker cyberresiliensen och cyberhygienen hos små och medelstora företag, särskilt de som inte omfattas av NIS 2-direktivet, genom att tillhandahålla lättillgänglig vägledning och stöd för deras specifika behov, i enlighet med artikel 7.2 i NIS 2-direktivet.

Syfte: Aktiviteten stödjer målet genom att ta fram riktlinjer som kan vara till gagn för små och medelstora företag som utvecklar sitt cybersäkerhetsarbete.

NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

6.2 Medel tillförs MCF för att intensifiera det brottsförebyggande samarbetet med Stöldskyddsföreningen.

Syfte: Genom att vidareutveckla arbetet med målgruppsanpassat stöd förstärks stödet till små och medelstora företag ytterligare.

MCF

2025–2027

Pelare B: Utvecklad kunskap och kompetensutveckling inom cybersäkerhet

Mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien hos allmänheten

7.1 Medel tillförs MCF för att vidareutveckla kampanjen ”Tänk säkert”.

Syfte: Aktiviteten stödjer målet genom att kampanjen syftar till att öka cybersäkerhetsmedvetenhetenen i samhället vilket långsiktigt bidrar till att höja lägstanivån och därmed motståndskraften mot såväl cyberattacker som andra hybridaktiviteter.

MCF

2025–2027

Mål 8: Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

8.1 Medel tillförs Cybercampus Sverige för att ytterligare stärka verksamheten.

Syfte: Aktiviteten stödjer målet genom att ge Cybercampus ökade förutsättningar att utgöra navet för utbildning, forskning och kompetensförsörjning inom hela cybersäkerhetsområdet.

Cybercampus vid Kungliga tekniska högskolan

2024–2028

8.2 Försvarsmakten, Säkerhetspolisen och Försvarshögskolan samarbetar kring kompetensförsörjning inom primärt säkerhetsskyddsområdet.

Syfte: Aktiviteten stödjer målet genom ett stärkt samarbete mellan aktörer som syftar till att avhjälpa brister i kompetensförsörjning på säkerhetsområdet.

Försvarsmakten, Säkerhetspolisen och Försvarshögskolan

Tills vidare

8.3 MCF fortsätter arbetet med kompetensförsörjning inom cybersäkerhet.

Syfte: Att stödja och sammanlänka med det arbete som sker på EU-nivå i europeiska kompetenscentrumet för cybersäkerhet (ECCC) rörande standardiserade roller, profiler och kompetenser inom cybersäkerhet.

MCF

Tills vidare

8.4 Mediemyndigheten fortsätter verka för medie- och informationskunnighet (MIK) och att samordna det nationella arbetet med MIK.

Syfte: Myndigheten har i uppgift att verka för MIK och att samordna arbetet med MIK i Sverige. De koordinerar ett nätverk bestående av 24 myndigheter och organisationer samt fyra kretsar för samverkan – Folkbildningsarenan för MIK, Interregionala MIK-nätverket, Akademiskt forum för MIK-forskning samt Mediearenan för MIK. Syftet med nätverket är att genom samverkan utveckla kunskap, stärka kvaliteten och effektivisera arbetet – och därigenom stärka medie- och informationskunnigheten hos alla i Sverige. Det är ett område i utveckling, eftersom teknik och medieanvändning ständigt förändras. Inom nätverket ansvarar myndigheten även för en kunskapsbank om MIK med informationsmaterial, forskningsrapporter och lärarhandledningar från olika verksamheter som är tillgängligt för alla.

Mediemyndigheten

Tills vidare

8.5 NCSC vid FRA och MCF ska inom ramen för NCSC ta fram riktlinjer för att främja och utveckla cybersäkerhetsutbildning, cybersäkerhetskompetens, medvetandehöjande åtgärder och forsknings- och utvecklingsinitiativ, samt vägledning om god praxis och kontroll för cyberhygien som riktar sig till medborgare, intressenter och entiteter, i enlighet med artikel 7.2 i NIS 2-direktivet.

Syfte: Aktiviteten stödjer målet genom att riktlinjer upprättas som bland annat berör centrala frågor för att främja ökad cybersäkerhetskompetens.

NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

Mål 9: Stärkt forskning och innovation på cybersäkerhetsområdet

9.1 MCF tillhandahåller ett nationellt samordningscenter (NCC-SE).

Syfte: NCC-SE stöttar EU:s kompetenscentrum för cybersäkerhet (ECCC), bidrar i framtagning av arbetsprogram på EU-nivå, marknadsför de europeiska cybersäkerhetsutlysningarna samt ger vägledning till svenska aktörer som söker EU-medel för projekt inom arbetsprogrammen från ECCC. Sammantaget bidrar aktiviteten till målet genom att ge förutsättning för stärkt forskning och innovation.

MCF

Tills vidare

9.2 Medel tillförs för stärkt forskning och innovation inom cybersäkerhet genom nationellt samordningscenter (NCC-SE).

Syfte: Genom att stärka NCC-SE, inklusive dess möjlighet att förvalta EU-medel som stöd till tredje part, ökas förutsättningarna för stärkt forskning och innovation på cybersäkerhetsområdet i Sverige.

MCF

2025–2027

9.3 Medel tillförs för MCF:s vidareutveckling av Cybernoden.

Syfte: Aktiviteten stödjer målet genom att den svenska Cybernodens arbete med att samla näringsliv, akademi och offentlig sektor utvecklas.

MCF

2025–2027

9.4 **Uppdaterad:** MCF beställer, kvalitetssäkrar och förmedlar forskning och utvecklingsarbete för skydd mot olyckor, krisberedskap och civilt försvar.

Syfte: Aktiviteten stödjer målet genom att MCF, inom ramen för myndighetens utlysningar inom civilt försvar och krisberedskap, också främjar forskning på cybersäkerhetsområdet.

MCF

Tills vidare

9.5 **Uppdaterad:** Medel tillförs Vetenskapsrådet för satsningar inom ett antal forskningsområden.

Syfte: Att stärka forskningen genom program inom:

- informations- och cybersäkerhet,
- digitaliseringens samhälleliga konsekvenser,
- säkra samhällen.

Vetenskapsrådet

2026

Mål 10: Stärkt förmåga att hantera framväxande teknologiers risker och möjligheter

10.1 **Uppdaterad:** Uppdrag till Mediemyndigheten att genomföra en nationell satsning för stärkt medie- och informationskunnighet i en tid av artificiell intelligens och desinformation.

Syfte: Aktiviteten stödjer målet genom att stärka individer som medvetna medieanvändare och även höja befolkningens kunskap om AI.

Mediemyndigheten

2024–2028

10.2 Regeringen gör en satsning som uppgår till drygt 1,2 miljarder kronor årligen från 2028 på excellenskluster för banbrytande teknik.

Syfte: Kvantteknik har potentialen att revolutionera databehandling, simulering, sensorer och kommunikation och lösa problem som dagens datorer inte kan hantera. Denna breda satsning syftar till att täcka in såväl forskning på teknik i ett tidigt skede som innovation och tillämpning i ett senare skede av teknikutvecklingen, och går därför via både Vetenskapsrådet och Vinnova.

Vetenskapsrådet och Vinnova

2024–2028

10.3 Försvarsmakten deltar i samarbete och aktiviteter som bedrivs inom EU:s och Natos arbetsgrupper för krypto och relevanta standardiseringsforum. I dessa sammanhang ska myndigheten bland annat söka få genomslag för svenska ståndpunkter och verka för att policy och regelverk är praktiskt genomförbart, ger ett adekvat skydd och tar hänsyn till kvantdatorhotet.

Syfte: Aktiviteten stödjer målet genom att söka öka svensk förmåga att hantera risker kopplade till framtida kvantutveckling och kvantdatorer.

Försvarsmakten med stöd av FRA

Tills vidare

10.4 Försvarsmakten undersöker förutsättningarna för att anpassa krav och utveckling av kommande signalskyddssystem efter Natos policy, krav och interoperabilitetsspecifikationer.

Syfte: Aktiviteten stödjer målet genom att bidra till utvecklad svensk kompetens och förmåga inom signalskydd.

Försvarsmakten

Tills vidare

10.5 **Ny:** Regeringen har beslutat om Sveriges digitaliseringsstrategi 2025–2030.

Syfte: Digitaliseringsstrategin anger en tydlig inriktning för regeringens digitaliseringspolitik genom att identifiera utmaningar och ange målsättningar inom ett antal strategiskt viktiga områden. Regeringens målsättning är att Sverige ska ha hög digital motståndskraft och tillförlitlighet för att användare och tjänster ska vara säkra och information ska vara säker. Strategin ramar också in regeringens arbete med att bland annat skapa robust, resilient och redundant digital infrastruktur, vilket också främjar en stärkt cybersäkerhet.

Regeringen

2025–2030

10.6 **Ny:** Regeringen har beslutat om Sveriges AI-strategi.

Syfte: Strategin syftar till att säkerställa att Sverige snabbt drar nytta av de stora möjligheter som AI-utvecklingen innebär. Strategin identifierar även risker som AI för med sig och som är relevanta ur bland annat ett cybersäkerhetsperspektiv.

Regeringen

2026

Pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter

Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt

11.1 NCSC vid FRA främja samverkan med privata och offentliga aktörer.

Syfte: Stärkt privat-offentlig samverkan skapar förutsättningar för bland annat effektivare informationsdelning.

NCSC vid FRA i samverkan med FMV, Försvarsmakten, MCF, Polismyndigheten, PTS och Säkerhetspolisen

Tills vidare

11.2 NCSC tar fram lägesbilder avseende cyberhot och incidenter

Syfte: Aktiviteten stödjer målet genom att lägesbilder avseende aktuella cyberhot och incidenter tas fram för näringslivet, kommuner och regioner, myndigheter samt Regeringskansliet och därmed stöttar aktörer i att förstå hotbilden på såväl cyber- som hybridområdet.

NCSC vid FRA i samverkan med FMV, Försvarsmakten, MCF, Polismyndigheten, PTS och Säkerhetspolisen

Tills vidare

11.3 NCSC vid FRA och MCF ska ta fram riktlinjer inbegripet relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan entiteter i enlighet med unionsrätten i enlighet med artikel 7.2 i NIS 2-direktivet.

Syfte: Riktlinjer rörande frivilligt informationsutbyte om cybersäkerhet bidrar till effektiv informationsdelning.

NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

11.4 NCSC vid FRA och MCF ska inom ramen för NCSC ta fram riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter enligt NIS 2-direktivets artikel 12.1 i enlighet med artikel 7.2 NIS 2-direktivet.

Syfte: Aktiviteten stödjer målet genom att adressera delning av information om sårbarheter, vilket utgör en viktig aspekt av effektiv informationsdelning.

NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

11.5 Berörda statliga myndigheter fortsätter att inom ramen för årsrapporter informera om hotbilden inom sina respektive sakområden.

Syfte: Myndigheternas olika perspektiv i rapporterna stödjer målet genom att utgöra ett viktigt bidrag i informationsdelning från statliga myndigheter som organisationer kan nyttja för att skapa sig en god lägesbild.

FRA, Försvarsmakten, MCF, Säkerhetspolisen, Polismyndigheten, FMV och PTS

Tills vidare

11.6 **Ny:** MCF erbjuder genom CERT-SE automatiska notifieringar av tekniska sårbarheter (ANTS) till svenska verksamheter.

Syfte: Genom att utveckla och tillhandahålla ANTS stärks svenska verksamheters förmåga att övervaka angreppsytor och förebygga cybersäkerhetsincidenter.

MCF

Tills vidare

11.7 **Ny:** MCF erbjuder genom CERT-SE en nationell plattform för svenska verksamheter att dela och ta del av hotinformation (MISP, malware information sharing platform).

Syfte: Aktiviteten hjälper användare att dela hotindikatorer för att snabbt reagera på nya hot och stärka Sveriges samlade motståndskraft mot cyberangrepp genom delning av hotinformation.

MCF

Tills vidare

11.8 **Ny:** MCF utses till nationellt cybernav i enlighet med cybersolidaritetsförordningen.

Syfte: MCF får möjlighet att delta i det europeiska nätverket för cybersäkerhetsvarningar.

MCF

Till och med 30 juni 2026

11.9 **Ny:** NCSC vid FRA deltar i det myndighetsgemensamma arbetet och stödjer relevanta aktörer i frågor om cybersäkerhet inför, under och efter genomförandet av valen till riksdag, region- och kommunfullmäktige 2026.

Syfte: Aktiviteten stärker det cybersäkerhetsrelaterade stöd som berörda aktörer kan ta del under valåret 2026 för att skydda valens genomförande.

NCSC vid FRA med stöd av MCF, FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2026

Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter

12.1 FRA fortsätter erbjuda tekniskt stöd, inklusive detekterings- och varningssystem (TDV), till de mest skyddsvärda verksamheterna.

Syfte: Genom att utveckla och tillhandahålla tekniskt stöd, inklusive TDV, stärks de mest skyddsvärda verksamheternas förmåga att förebygga och upptäcka cybersäkerhetsincidenter. cybersäkerhetsincidenter.

FRA

Tills vidare

12.2 Nationell informationssäkerhetsövning (NISÖ) fortsätter att genomföras inom ramen för NCSC.

Syfte: Aktiviteten stödjer målet genom att ge privata och offentliga aktörer möjlighet att öva tillsammans och därigenom stärka samhällets samlade förmåga att hantera it-relaterade samhällsstörningar där skyndsam samordning krävs.

MCF i samverkan med berörda aktörer

Tills vidare

12.3 Statliga myndigheter genomför nationella cybersäkerhetsövningar inom ramen för NCSC vid FRA.

Syfte: Aktiviteten stödjer målet genom övningar som bland annat berör incidenthantering och bidrar till att stärka Sveriges förmåga att förebygga, upptäcka och hantera cyberhot och cyberangrepp.

NCSC vid FRA i samverkan med FMV, Försvarsmakten, MCF, Polismyndigheten, PTS och Säkerhetspolisen

Tills vidare

12.4 **Uppdaterad:** MCF fortsätter att planera, genomföra, utvärdera cybersäkerhetsövningar, inklusive att tillsammans med Försvarsmakten och Totalförsvarets forskningsinstitut (FOI) utveckla nationell Cyber Range.

Syfte: Genom att stärka det kollektiva lärandet höjs privata och offentliga organisationers incidenthanteringsförmåga.

MCF, Försvarsmakten, Totalförsvarets forskningsinstitut (FOI)

Tills vidare

12.5 **Uppdaterad:** MCF skapar, i samverkan med FRA/NCSC, en nationell portal för anmälan, rapportering och stöd, primärt utifrån kraven i NIS 2- och CER-direktiven.

Syfte: Att göra det lätt utföra sin plikt respektive att kräva sin rätt enligt kraven i både cybersäkerhetslagen (CSL) och lagen om motståndskraft hos kritiska verksamhetsutövare (LMV) genom att:

1. möjliggöra samlad anmälan av verksamhetsutövare enligt kraven i både CSL och LMV, inklusive anmälan till tjänsten ANTS,

2. möjliggöra rapportering enligt kraven i både CSL och LMV i en och samma tjänst,

3. införa möjlighet till ökat informationsutbyte och ytterligare funktionalitet för både rapporterande och mottagande organisationer,

4. införa möjlighet att begära sådant stöd som verksamhetsutövare enligt CSL och LMV har rätt till,

5. ge samlad tillgång till stödtjänster som Cybersäkerhetsrådgivningen, Metodstödet för cybersäkerhet och Cybersäkerhetskollen.

I ett första skede möjliggörs anmälan och rapportering. Ytterligare tjänster utvecklas över tid. På sikt är portalen tänkt att kunna omhänderta krav på rapportering i enlighet med annan ytterligare lagstiftning.

MCF

Tills vidare

12.6 MCF fortsätter arbetet med årsrapporter om it-incidenter.

Syfte: Aktiviteten stödjer målet genom att incidenter som rapporterats in till den statliga myndigheten sammanställs och analyseras över tid vilket möjliggör att följa trender kring cybersäkerhetsincidenter samt för organisationer att dra lärdomar till sin incidenthanteringsförmåga.

MCF

Tills vidare

12.7 NCSC vid FRA och MCF ska ta fram riktlinjer för att främja ett aktivt cyberskydd, i enlighet med artikel 7.2 i NIS 2-direktivet.

Syfte: Aktiviteten stödjer målet genom att främja ett aktivt cyberskydd, vilket organisationer kan använda för att stärka sin förmåga att hantera och bemöta cybersäkerhetsincidenter.

NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

2025–2026

12.8 Polismyndigheten ser över förutsättningarna att etablera en process för ökat samarbete kring incidentrapportering.

Syfte: Aktiviteten stödjer målet genom att se över förutsättningarna att mer effektivt nyttja statliga myndigheters samlade utredande, hanterande och förebyggande resurser på cybersäkerhetsområdet för att förebygga eller lagföra cyberbrott.

Polismyndigheten

Tills vidare

12.9 Inom ramen för Nationella telesamverkansgruppens (NTSG) krisberedskapsövningar övar aktörer inom elektroniska kommunikationer på cyberincidenter när så är lämpligt.

Syfte: Aktörer inom elektronisk kommunikation utvecklar bättre rutiner och färdigheter i hanteringen av cybersäkerhetsrelaterade risker.

PTS

Tills vidare

12.10 **Genomförd:** FRA ska utarbeta en nationell operativ plan för storskaliga cybersäkerhetsincidenter och kriser i enlighet med artikel 9 i NIS 2-direktivet.

Syfte: En operativ plan om storskaliga incidenter och kriser är en central del i att utveckla Sveriges samlade förmåga att snabbt och effektivt kunna hantera sådana incidenter och kriser.

MSB och FRA

2025

12.11 **Uppdaterad:** MCF är cyberkrishanteringsmyndighet med ansvar för att samordna hanteringen av storskaliga cybersäkerhetsincidenter och kriser enligt artikel 9.1 och CSIRT-enhet enligt artikel 10.1 NIS 2-direktivet. Myndigheten företräder Sverige i EU-CyCLONe och CSIRT-nätverket.

Syfte: Att utse behörig myndighet med ansvar för vissa uppgifter enligt NIS 2-direktivet.

MCF

Tills vidare

12.12 Medel tillförs MCF för utveckling av stärkt operativ cybersäkerhetsförmåga.

Syfte: Att stärka funktionen CERT-SE och utveckla förmågan att erbjuda kvalificerat stöd till drabbade aktörer samt fortsätta att bygga förmåga att hantera cyberangrepp.

MCF

2025–2027

12.13 MCF verkar för att privata och offentliga organisationer ges tillgång till och kan nyttja det tekniska och organisatoriska stöd som tillhandahålls på EU-nivå för att stärka motståndskraften mot storskaliga cyberattacker.

Syfte: Att dra nytta av det stöd som bland annat ENISA tillhandahåller i syfte att stärka organisationers möjlighet att förebygga och hantera storskaliga cyberattacker.

MCF

Tills vidare

12.14 **Ny:** Den nationella planen för hantering av storskaliga cybersäkerhetsincidenter och kriser är utgångspunkten för nationell operativ incidenthantering. FRA håller planen uppdaterad.

Syfte: Att upprätthålla en aktörsgemensam uppfattning om hur storskaliga cybersäkerhetsincidenter ska hanteras på nationell nivå och bidra till effektiv samverkan mellan cyberkrishanteringsmyndigheten (MCF), NCSC och samverkansmyndigheterna.

FRA i samverkan med MCF, FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen

Tills vidare

12.15 **Ny och genomförd:** Regeringen har gett Myndigheten för samhällsskydd och beredskap (MSB) och Post- och telestyrelsen (PTS) i uppdrag att förbereda genomförandet av NIS 2-direktivet.

Syfte: Uppdragen gavs för att skapa förutsättningar för en effektiv nationell implementering av NIS 2-direktivet.

Regeringen

2025

Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott

13.1 Polismyndigheten fortsätter att fördjupa sitt samarbete med andra säkerhets- och brottsbekämpande myndigheter samt relevanta privata aktörer.

Syfte: Aktiviteten stödjer målet genom operativt samarbete som ökar förmågan att bekämpa cyberbrott.

Polismyndigheten

Tills vidare

13.2 **Uppdaterad:** MCF är nationell gemensam kontaktpunkt i enlighet med NIS 2-direktivet.

Syfte: Genom rollen som nationell gemensam kontaktpunkt bidrar MCF till målet genom att bland annat säkerställa samarbete mellan brottsbekämpande myndigheter och dataskyddsmyndigheter.

MCF

2025

13.3 Polismyndigheten deltar i samarbete med finans- och transaktionsmarknaderna i arbetet för säkrare betalningar

Syfte: Att förebygga cyberbrott inom transaktionssystemen.

Polismyndigheten

Tills vidare

13.4 Polismyndigheten deltar i brottsförebyggande nätverk gällande cyberbrott.

Syfte: Att genom bred samverkan öka förmågan att förebygga cyberbrott.

Polismyndigheten

Tills vidare

13.5 Polismyndigheten deltar i brottsförebyggande samarbete med Stöldskyddsföreningen och andra aktörer. Arbetet innefattar att genom säkerhetskollen.se ge varningar till allmänheten om pågående bedrägeritrender, att via ett kunskapscenter med MCF och flera andra statliga myndigheter skapa bland annat medvetandehöjande kampanjer och helpdesk samt att genom digitala varningsgruppen fortsätta det brottsförebyggande arbetet.

Syfte: Att genom samarbete stärka förutsättningarna att skydda allmänheten samt små och medelstora företag och därigenom öka förmågan att förebygga och bekämpa cyberbrott.

Polismyndigheten, MCF och Stöldskyddsföreningen

Tills vidare

13.6 Polismyndigheten fördjupar fortsatt samarbetet med Europol avseende brottsförebyggande arbete.

Syfte: Genom ökad användning av det material och de aktiviteter som Europol erbjuder, bland annat under European Cyber Security Month (ECSM), bidrar aktiviteten till arbetet med att förebygga cyberbrott.

Polismyndigheten

Tills vidare

13.7 Polismyndigheten deltar fortsatt i Europols Joint Cybercrime Action Taskforce.

Syfte: Aktiviteten stödjer målet genom att fördjupa det internationella samarbetet med statliga myndigheter och privata aktörer avseende utredning av cyberbrott.

Polismyndigheten

Tills vidare

13.8 Polismyndigheten utvecklar sin förmåga att bekämpa cyberbrott.

Syfte: Aktiviteten stödjer målet genom att öka förmågan att utreda inträffade cyberbrott samt förmågan att säkra bevismaterial i digitala miljöer.

Polismyndigheten

Tills vidare

13.9 **Ny:** Polismyndigheten har inrättat en permanent nationell cyberinsatsstyrka vid Nationellt IT-brottscentrum.

Syfte: Den nationella cyberinsatsstyrkan har utvecklats som ett projekt som planeras bli permanent under 2026. Den nationella cyberinsatsstyrkan har till uppdrag att ingripa, störa och avbryta allvarliga cyberangrepp och säkra bevisning samt bistå med specialiserad cyberkompetens vid insatser mot organiserad brottslighet.

Polismyndigheten

2026

13.10 **Ny:** Regleringen om hemliga och preventiva tvångsmedel ses över inom ramen för en särskild utredning (Utredningen om hemliga och preventiva tvångsmedel, Ju2025:04). Ett deluppdrag tar sikte på att utreda och föreslå en möjlighet att störa och avbryta pågående brott eller brottslig verksamhet i cybermiljö för att förbättra de brottsbekämpande myndigheternas samlade förmåga att ingripa mot sådan brottslighet.

Syfte: Aktiviteten stödjer målet genom att fördjupa det internationella samarbetet med statliga myndigheter och privata aktörer avseende utredning av cyberbrott.

Hemliga och preventiva tvångsmedel – en effektiv och tydlig reglering (Dir. 2025:12)

2025–2026, uppdraget ska redovisas senast den 29 maj 2026

13.11 **Ny:** Lagrådsremiss för att genomföra EU:s e-bevisningspaket, SOU 2024:85 Effektivare gränsöverskridande inhämtning av elektroniska bevis.

Syfte: Aktiviteten stödjer målet genom att öka förmågan att utreda inträffade cyberbrott samt förmågan att säkra bevismaterial i digitala miljöer.

Regeringen

2025–2026

Förteckning över aktiviteter

Här följer en överskådlig lista på samtliga aktiviteter i handlingsplanen.

Pelare A: Systematiskt och effektivt cybersäkerhetsarbete

Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer

#	Aktivitet	Ansvarig*	Tid	Hänvisning
1.1	Nationellt cybersäkerhets-centers (NCSC) verksamhet inom Försvarets radioanstalt (FRA) bedrivs utifrån en ny förordning.	Regeringen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
1.2	**Uppdaterad:** CER-direktivet genomförs nationellt på ett harmoniserat sätt.	Regeringen	2026	Europaparlamentets och rådets direktiv (EU) 2022/2557 av den 14 december 2022 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet)
1.3	**Uppdaterad:** Remittering och beredning av förslagen i betänkandet Kompletterande bestämmelser till EU:s cyberresiliensförordning.	Fi 2024:07	2026	Dir 2024:119 och Kompletterande bestämmelser till EU:s cyberresiliensförordning (SOU 2025:115) Remiss av SOU 2025:115 Kompletterande bestämmelser till EU:s cyberresiliensförordning (Fi2026/00065)
1.4	**Uppdaterad:** Myndigheten för civilt försvar (MCF) säkerställer att ett utbildningsutbud finns tillgängligt för organisationer som omfattas av NIS 2-direktivet och beredskapssektorerna.	MCF	2024–2027	Budgetpropositionen 2025
1.5	NCSC vid FRA och MCF ska inom ramen för NCSC ta fram riktlinjer för att främja utveckling och integrering av relevant avancerad teknik som syftar till att genomföra moderna riskhanteringsåtgärder för cybersäkerhet i enlighet med artikel 7.2 i NIS 2-direktivet.	NCSC vid FRA och MCF med bistånd av Försvarets materielverk (FMV), Försvarsmakten, Polismyndigheten, Post- och telestyrelsen (PTS) och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)

* Regeringen har gett Försvarets radioanstalt (FRA) och Myndigheten för civilt försvar (MCF) i uppdrag att förbereda överföring av cybersäkerhetsverksamheten vid MCF till Nationellt cybersäkerhets-centrum (NCSC) inom FRA. Överföringen ska ske den 1 juli 2026. Det innebär att ansvaret för huvuddelen av de aktiviteter i handlingsplanen som står på MCF överförs till FRA vid denna tidpunkt.

1.6	MCF fortsätter utveckla och förvalta råd och stöd för organisationers systematiska cybersäkerhetsarbete.	MCF	Tills vidare	Förordning med instruktion för MCF
1.7	MCF fortsätter arbetet med analyser och temarapporter inom cybersäkerhetsområdet.	MCF	Tills vidare	Förordning med instruktion för MCF EU-finansierat projekt ENIAC
1.8	Finansinspektionen fortsätter utöva tillsyn över den finansiella sektorns cybersäkerhetsarbete och digitala operativa motståndskraft.	Finansinspektionen	Tills vidare	Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA)
1.9	MCF vidareutvecklar Cybersäkerhetskollen för att kunna bistå fler organisationer i fler processer och kunna förmedla en fördjupad nationell lägesbild kring cybersäkerhetsnivån i samhällsviktiga verksamheter.	MCF	2025–2027	Budgetpropositionen 2025
1.10	**Ny:** Vetenskapsrådet ska ta fram och fastställa riktlinjer i syfte att ge stöd till lärosäten, forskningsinstitut och forskningsfinansiärer för att utveckla, förbättra och främja användningen av cybersäkerhetsverktyg och säker nätinfrastruktur i enlighet med artikel 7.2 i NIS 2-direktivet.	Vetenskapsrådet	2026	Regleringsbrev (U2025/01357)
1.11	**Ny:** Naturvårdsverket tillförs medel.	Naturvårdsverket	2026	Budgetpropositionen 2026
1.12	**Ny:** Energimyndigheten tillförs medel.	Energimyndigheten	Tills vidare	Budgetpropositionen 2026
1.13	**Ny:** Överföring av uppgifter på cybersäkerhetsområdet från MCF till NCSC vid FRA.	MCF och NCSC vid FRA	2026	Regeringsuppdrag den 20 november 2025 Fö nr II:1 (Fö2025/01703) och Fö nr II:2 (Fö2025/01704)
1.14	**Ny:** NCSC vid FRA tillförs medel.	Regeringen	Tills vidare	Budgetpropositionen 2026
1.15	**Ny:** NCSC vid FRA ska genomföra mätning av resultatindikatorer.	NCSC vid FRA	2026	Regeringsuppdrag Fö2025/01547

Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering

#	Aktivitet	Ansvarig*	Tid	Hänvisning
2.1	MCF ska med stöd av FRA och FMV genomföra en nationell kartläggning av kommuners tekniska cybersäkerhetsförmåga. Kartläggningen ska ske genom upphandlade it-säkerhetsanalyser utförda av privata företag.	MCF med stöd av FRA och FMV	2025–2027	Budgetpropositionen 2025 Regeringsuppdrag den 20 mars 2025 Fö nr II:2 (Fö 2025/00540)

2.2	Över 100 myndigheter implementerar uppdrag att redogöra för hur de förvaltat och utvecklat sitt arbete med informations- och cybersäkerhet.	Berörda statliga myndigheter	2025–2026	Regleringsbrev
2.3	MCF etablerar en kompletterande analysmiljö till Cybersäkerhetskollen där drift, förvaltning och utveckling ingår.	MCF	2025–2027	Budgetpropositionen 2025
2.4	**Uppdaterad:** NCSC vid FRA och MCF ska ta fram riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för produkter inom informations- och kommunikationsteknik (IKT), IKT-tjänster, IKT-processer och utlokaliserade säkerhetstjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhets-certifiering, kryptering och användning av cybersäkerhets-produkter med öppen källkod i enlighet med artikel 7.2 i NIS 2-direktivet.	NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)
2.5	**Uppdaterad:** Regeringskansliet uppdaterar strategins bilaga 2, ”Organisationer med roller och ansvarsområden inom cybersäkerhet”, när organisations-förändringar och ansvarsfördelning trätt i kraft i enlighet med aktivitet 1:13 i denna handlingsplan.	Regeringskansliet	2026	Budgetpropositionen 2026
2.6	**Genomförd:** Uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet.	Fö 2024:04	2024–2025	Dir. 2024:111
2.7	**Ny:** Försäkringskassan, Lantmäteriet, Skatteverket och Trafikverket erbjuder it-driftstjänster inom ett samordnat statligt tjänsteutbud och tillhandahåller dessa till intresserade myndigheter.	Försäkringskassan, Skatteverket, Trafikverket, Lantmäteriet	Tills vidare	Förordning (2024:1005) om samordnad och säker statlig it-drift

Mål 3: Stärkt säkerhetsarbete inom kritisk infrastruktur

#	Aktivitet	Ansvarig	Tid	Hänvisning
3.1	MCF tillhandahåller stöd för samhällsviktig verksamhets arbete med säkerhet i operativ teknik (OT).	MCF	Tills vidare	Förordning med instruktion för MCF
3.2	NCSC vid FRA och MCF ska ta fram riktlinjer för att upprätthålla den allmänna tillgängligheten, integriteten och konfidentialiteten hos den offentliga kärnan i det öppna internet. Inbegripet, i tillämpliga fall, cybersäkerheten hos undervattenskablar i enlighet med artikel 7.2 i NIS 2-direktivet.	FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/000389)
3.3	Hotbildsstyrda penetrationstester genomförs regelbundet på organisationer inom den finansiella sektorn.	Finansinspektionen och Sveriges Riksbank	Tills vidare	Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn Lag (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn

Mål 4: Robustare digitala leveranskedjor och minskat beroende

#	Aktivitet	Ansvarig	Tid	Hänvisning
4.1	Berörda statliga myndigheter fortsätter bidra till standardisering av cybersäkerhet inom ramen för NCSC-samverkan.	PTS och FMV i samverkan med Försvarsmakten, FRA, MCF Säkerhetspolisen och Polis-myndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
4.2	FMV deltar i samarbeten och aktiviteter som bedrivs inom ramen för EU:s ramverk för cybersäkerhets-certifiering. I dessa sammanhang ska myndigheten bland annat söka få genomslag för svenska ståndpunkter och verka för att nya certifieringsordningar tas fram på ett transparent sätt.	FMV	Tills vidare	Lagen (2021:553) med kompletterande bestämmelser till EU:s cybersäkerhetsakt Förordning (2021:555) med kompletterande bestämmelser till EU:s cybersäkerhetsakt Övergripande instruktion vid förhandling enligt det europeiska ramverket för cybersäkerhetscertifiering
4.3	MCF genomför en kartläggning av digitala leveranskedjor och tar fram en modell för uppföljning av digitala leveranskedjor.	MCF	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:5 (Fö2025/000390)
4.4	NCSC vid FRA och MCF ska ta fram riktlinjer för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter när de tillhandahåller sina tjänster, i enlighet med artikel 7.2 i NIS 2-direktivet.	NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhets-polisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/000389)

Mål 5: Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete

#	Aktivitet	Ansvarig	Tid	Hänvisning
5.1	**Uppdaterad:** MCF är nationell gemensam kontaktpunkt i enlighet med NIS 2-direktivet.	MCF	2025	Cybersäkerhetslagen (2025:1506) Cybersäkerhetsförordningen (2025:1507)
5.2	Berörda statliga myndigheter fortsätter inom ramen för NCSC-samverkan arbetet med en nationell modell där föreskrifter, allmänna råd och vägledningar så långt som möjligt ensas så att de följer en likartad logik, struktur och terminologi.	NCSC vid FRA, Försvarsmakten, MCF, Säkerhets-polisen och FMV	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
5.3	Medel tillförs ett antal statliga myndigheter för att förbereda och utveckla sin tillsynsverksamhet utifrån NIS 2-direktivet.	Vissa länsstyrelser, Läkemedelsverket, Inspektionen för vård och omsorg, Transportstyrelsen, Livsmedelsverket, Statens energimyndighet och PTS	Tills vidare	Budgetpropositionen 2025
5.4	Säkerhetspolisen och Försvarsmakten utvecklar löpande tillsynsverksamheten kring, och samarbetet mellan, myndigheter som har ansvar enligt säkerhetsskydds-lagstiftningen.	Säkerhetspolisen och Försvarsmakten	Tills vidare	Förordningar med myndigheternas instruktioner Säkerhetsskyddslag (2018:585) Säkerhetsskyddsförordning (2021:955)
5.5	Säkerhetspolisen och Försvarsmakten utvecklar kontinuerligt stödjande material såsom vägledningar, handböcker och utbildningsmaterial inom säkerhetsskydd.	Säkerhetspolisen och Försvarsmakten	Tills vidare	Förordningar med myndigheternas instruktioner Säkerhetsskyddslag (2018:585) Säkerhetsskyddsförordning (2021:955)
5.6	MCF förvaltar, utvecklar och tillhandahåller publik databas över svensk terminologi inom cybersäkerhetsområdet.	MCF	Tills vidare	Förordning med instruktion för MSB
5.7	MCF tillhandahåller och vidareutvecklar rådgivningstjänst med särskilt fokus på NIS 2-aktörer.	MCF	2025–2027	Förordning med instruktion för MCF Budgetpropositionen 2025
5.8	**Ny:** Regioner tillförs medel för ökad cybersäkerhet.	Regioner	Tills vidare	Budgetpropositionen 2026
5.9	**Ny:** Kommuner tillförs medel för ökad cybersäkerhet.	Kommuner	Tills vidare	Budgetpropositionen 2026
5.10	**Ny:** Svenska lärosäten tilldelas medel för ökad cybersäkerhet och för implementering av cybersäkerhetslagen.	Lärosäten	Tills vidare	Budgetpropositionen 2026

Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete

#	Aktivitet	Ansvarig	Tid	Hänvisning
6.1	NCSC vid FRA och MCF ska inom ramen för NCSC ta fram riktlinjer som stärker cyberresiliensen och cyberhygienen hos små och medelstora företag, särskilt de som inte omfattas av NIS 2-direktivet, genom att tillhandahålla lättillgänglig vägledning och stöd för deras specifika behov, i enlighet med artikel 7.2 i NIS 2-direktivet.	NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/000389)
6.2	Medel tillförs MCF för att intensifiera det brottsförebyggande samarbetet med Stöldskyddsföreningen.	MCF	2025–2027	Budgetpropositionen 2025

Pelare B: Utvecklad kunskap och kompetensutveckling inom cybersäkerhet

Mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien hos allmänheten

#	Aktivitet	Ansvarig	Tid	Hänvisning
7.1	Medel tillförs MCF för att vidareutveckla kampanjen ”Tänk säkert”.	MCF	2025–2027	Budgetpropositionen 2025

Mål 8: Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

#	Aktivitet	Ansvarig	Tid	Hänvisning
8.1	Medel tillförs Cybercampus Sverige för att ytterligare stärka verksamheten.	Cybercampus vid Kungliga tekniska högskolan	2024–2028	Budgetpropositionen 2024 Forskning och innovation för framtid, nyfikenhet och nytta (prop. 2024/25:60)
8.2	Försvarsmakten, Säkerhetspolisen och Försvarshögskolan samarbetar kring kompetensförsörjning inom primärt säkerhetsskyddsområdet.	Försvarsmakten, Säkerhetspolisen och Försvars-högskolan	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
8.3	MCF fortsätter arbetet med kompetensförsörjning inom cybersäkerhet.	MCF	Tills vidare	Förordning med instruktion för MCF
8.4	Mediemyndigheten fortsätter verka för medie- och informationskunnighet (MIK) och att samordna det nationella arbetet med MIK.	Mediemyndigheten	Tills vidare	Förordning med instruktion för Mediemyndigheten

8.5	NCSC vid FRA och MCF ska inom ramen för NCSC ta fram riktlinjer för att främja och utveckla cybersäkerhetsutbildning, cybersäkerhetskompetens, medvetandehöjande åtgärder och forsknings- och utvecklingsinitiativ, samt vägledning om god praxis och kontroll för cyberhygien som riktar sig till medborgare, intressenter och entiteter, i enlighet med artikel 7.2 i NIS 2-direktivet.	NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/000389)

Mål 9: Stärkt forskning och innovation på cybersäkerhetsområdet

#	Aktivitet	Ansvarig	Tid	Hänvisning
9.1	MCF tillhandahåller ett nationellt samordnings-center (NCC-SE).	MCF	Tills vidare	Förordning med instruktion för MCF Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum
9.2	Medel tillförs för stärkt forskning och innovation inom cybersäkerhet genom nationellt samordnings-center (NCC-SE).	MCF	2025–2027	Budgetpropositionen 2025
9.3	Medel tillförs för MCF:s vidareutveckling av Cybernoden.	MCF	2025–2027	Budgetpropositionen 2025
9.4	**Uppdaterad:** MCF beställer, kvalitetssäkrar och förmedlar forskning och utvecklingsarbete för skydd mot olyckor, krisberedskap och civilt försvar.	MCF	Tills vidare	Förordning med instruktion för MCF
9.5	**Uppdaterad:** Medel tillförs Vetenskapsrådet för satsningar inom ett antal forskningsområden.	Vetenskapsrådet	2026	Kunskap i samverkan – för samhällets utmaningar och stärkt konkurrenskraft (prop. 2016/17:50) Forskning, frihet, framtid – kunskap och innovation för Sverige (prop. 2020/21:60) Forskning och innovation för framtid, nyfikenhet och nytta (prop. 2024/25:60) Myndighetens regleringsbrev

Mål 10: Stärkt förmåga att hantera framväxande teknologiers risker och möjligheter

#	Aktivitet	Ansvarig	Tid	Hänvisning
10.1	**Uppdaterad:** Uppdrag till Mediemyndigheten att genomföra en nationell satsning för stärkt medie- och informationskunnighet i en tid av artificiell intelligens och desinformation.	Mediemyndigheten	2024–2028	Regeringsuppdrag den 14 mars 2024 (Ku2024/00419) Myndighetens regleringsbrev
10.2	Regeringen gör en satsning som uppgår till drygt 1,2 miljarder kronor årligen till 2028 på excellenskluster för banbrytande teknik.	Vetenskapsrådet och Vinnova	2024–2028	Forskning och innovation för framtid, nyfikenhet och nytta (prop. 2024/25:60)
10.3	Försvarsmakten deltar i samarbete och aktiviteter som bedrivs inom EU:s och Natos arbetsgrupper för krypto och relevanta standardiseringsforum. I dessa sammanhang ska myndigheten bland annat söka få genomslag för svenska ståndpunkter och verka för att policy och regelverk är praktiskt genomförbart, ger ett adekvat skydd och tar hänsyn till kvantdatorhotet.	Försvarsmakten med stöd av FRA	Tills vidare	Uppgiften som kryptogodkännande myndighet (NCSA/CAA) Förordning med instruktion för Försvarsmakten
10.4	Försvarsmakten undersöker förutsättningarna för att anpassa krav och utveckling av kommande signalskyddssystem efter Natos policy, krav och interoperabilitets-specifikationer.	Försvarsmakten	Tills vidare	Uppgiften som kryptogodkännande myndighet (NCSA/CAA) Förordning med instruktion för Försvarsmakten
10.5	**Ny:** Regeringen har beslutat om Sveriges digitaliseringsstrategi 2025–2030.	Regeringen	2025–2030	Regeringsbeslut Fi2025/01181
10.6	**Ny:** Regeringen har beslutat om Sveriges AI-strategi.	Regeringen	2026	Regeringsbeslut Fi2026/00397

Pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter

Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt

#	Aktivitet	Ansvarig	Tid	Hänvisning
11.1	NCSC vid FRA ska främja samverkan med privata och offentliga aktörer.	NCSC vid FRA i samverkan med FMV, Försvarsmakten, MCF, Polis-myndigheten, PTS och Säkerhetspolisen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt

11.2	NCSC vid FRA tar fram lägesbilder avseende cyberhot och incidenter.	NCSC vid FRA i samverkan med FMV, Försvarsmakten, MCF, Polismyndigheten, PTS och Säkerhetspolisen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
11.3	NCSC vid FRA och MCF ska ta fram riktlinjer inbegripet relevanta förfaranden och lämpliga verktyg för informationsutbyte för att stödja ett frivilligt informationsutbyte om cybersäkerhet mellan entiteter i enlighet med unionsrätten i enlighet med artikel 7.2 i NIS 2-direktivet.	NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)
11.4	NCSC vid FRA och MCF ska inom ramen för NCSC ta fram riktlinjer för hantering av sårbarheter, inbegripet främjande och underlättande av samordnad delgivning av information om sårbarheter enligt NIS 2-direktivets artikel 12.1 i enlighet med artikel 7.2 i NIS 2-direktivet.	NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)
11.5	Berörda statliga myndigheter fortsätter att inom ramen för årsrapporter informera om hotbilden inom sina respektive sakområden.	FRA, Försvarsmakten, MCF, Säkerhetspolisen, Polismyndigheten, FMV och PTS	Tills vidare	Förordningar med myndigheternas instruktioner
11.6	**Ny:** MCF erbjuder genom CERT-SE automatiska notifieringar av tekniska sårbarheter (ANTS) till svenska verksamheter.	MCF	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
11.7	**Ny:** MCF erbjuder genom CERT-SE en nationell plattform för svenska verksamheter att dela och ta del av hotinformation (MISP, malware information sharing platform).	MCF	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
11.8	**Ny:** MCF utses till nationellt cybernav i enlighet med cybersolidaritets-förordningen.	MCF	Till och med 30 juni 2026	Regeringsuppdrag Fö2026/00231
11.9	**Ny:** NCSC vid FRA deltar i det myndighetsgemensamma arbetet och stödjer relevanta aktörer i frågor om cybersäkerhet inför, under och efter genomförandet av valen till riksdag, region- och kommunfullmäktige 2026.	NCSC vid FRA med stöd av MCF, FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2026	Regeringsuppdrag (Fö2025/01712)

Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter

#	Aktivitet	Ansvarig	Tid	Hänvisning
12.1	FRA fortsätter erbjuda tekniskt stöd, inklusive detekterings- och varningssystem (TDV), till de mest skyddsvärda verksamheterna.	FRA	Tills vidare	Förordning med instruktion för FRA
12.2	Nationell informations-säkerhetsövning (NISÖ) fortsätter att genomföras inom ramen för NCSC.	MCF i samverkan med berörda aktörer	Tills vidare	Förordning med instruktion för MCF
12.3	Statliga myndigheter genomför nationella cybersäkerhetsövningar inom ramen för NCSC vid FRA.	NCSC vid FRA i samverkan med FMV, Försvarsmakten, MCF, Polis-myndigheten, PTS och Säkerhetspolisen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
12.4	**Uppdaterad:** MCF fortsätter att planera, genomföra, utvärdera cybersäkerhetsövningar, inklusive att tillsammans med Försvarsmakten och Totalförsvarets forskningsinstitut (FOI) utveckla nationell Cyber Range.	MCF, Försvarsmakten och FOI	Tills vidare	Förordning med instruktion för MCF
12.5	**Uppdaterad:** MCF skapar, i samverkan med FRA/NCSC, en nationell portal för anmälan, rapportering och stöd, primärt utifrån kraven i NIS 2- och CER-direktiven.	MCF	Tills vidare	EU-finansierat projekt ENIAC
12.6	MCF fortsätter arbetet med årsrapporter om it-incidenter.	MCF	Tills vidare	Förordning med instruktion för MCF
12.7	NCSC vid FRA och MCF ska ta fram riktlinjer för att främja ett aktivt cyberskydd, i enlighet med artikel 7.2 i NIS 2-direktivet.	NCSC vid FRA och MCF med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)
12.8	Polismyndigheten ser över förutsättningarna att etablera en process för ökat samarbete kring incidentrapportering.	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndighetens ordinarie uppgifter
12.9	Inom ramen för Nationella telesamverkansgruppens (NTSG) krisberedskaps-övningar övar aktörer inom elektroniska kommunikationer på cyberincidenter när så är lämpligt.	PTS	Tills vidare	Proposition 2023/24:60 En telesamverkansgrupp för fredstida kriser och höjd beredskap
12.10	**Genomförd:** FRA ska utarbeta en nationell operativ plan för storskaliga cybersäkerhetsincidenter och kriser i enlighet med artikel 9 i NIS 2-direktivet.	MSB och FRA	2025	Regeringsuppdrag den 27 februari 2025 Fö nr II:2 (Fö2025/00388)

12.11	**Uppdaterad:** MCF är cyberkrishanterings-myndighet med ansvar för att samordna hanteringen av storskaliga cybersäkerhets-incidenter och kriser enligt artikel 9.1 och CSIRT-enhet enligt artikel 10.1 NIS 2-direktivet. Myndigheten företräder Sverige i EU-CyCLONe och CSIRT-nätverket.	MCF	Tills vidare	Cybersäkerhetslagen (2025:1506) Cybersäkerhetsförordningen (2025:1507)
12.12	Medel tillförs MCF för utveckling av stärkt operativ cybersäkerhetsförmåga.	MCF	2025–2027	Budgetpropositionen 2025
12.13	MCF verkar för att privata och offentliga organisationer ges tillgång till och kan nyttja det tekniska och organisatoriska stöd som tillhandahålls på EU-nivå för att stärka motståndskraften mot storskaliga cyberattacker.	MCF	Tills vidare	Förordning med instruktion för MCF Enisa Support Action
12.14	**Ny:** Den nationella planen för hantering av storskaliga cybersäkerhets-incidenter och kriser är utgångspunkten för nationell operativ incidenthantering. FRA håller planen uppdaterad.	FRA i samverkan med MCF, FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	Tills vidare	Nationell operativ plan för hantering av storskalig cybersäkerhetsincident och kris Artikel 9.4 i NIS 2-direktivet Regeringsuppdrag den 27 februari 2025 Fö nr II:2 (Fö2025/00388)
12.15	**Ny och genomförd:** Regeringen har gett Myndigheten för samhällsskydd och beredskap (MSB) och Post- och telestyrelsen (PTS) i uppdrag att förbereda genomförandet av NIS 2-direktivet.	Regeringen	2025	Regeringsuppdrag den 4 september 2025 (Fö2025/01293 respektive Fi2025/01676)

Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott

#	Aktivitet	Ansvarig	Tid	Hänvisning
13.1	Polismyndigheten fortsätter att fördjupa sitt samarbete med andra säkerhets- och brottsbekämpande myndigheter samt relevanta privata aktörer.	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndighetens ordinarie uppgifter
13.2	**Uppdaterad:** MCF är nationell gemensam kontaktpunkt i enlighet med NIS 2-direktivet.	MCF	2025	Cybersäkerhetslagen (2025:1506) Cybersäkerhetsförordningen (2025:1507)

13.3	Polismyndigheten deltar i samarbete med finans- och transaktionsmarknaderna i arbetet för säkrare betalningar.	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
13.4	Polismyndigheten deltar i brottsförebyggande nätverk gällande cyberbrott.	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
13.5	Polismyndigheten deltar i brottsförebyggande samarbete med Stöldskyddsföreningen och andra aktörer. Arbetet innefattar att genom säkerhetskollen.se ge varningar till allmänheten om pågående bedrägeritrender, att via ett kunskapscenter med MCF och flera andra statliga myndigheter skapa bland annat medvetandehöjande kampanjer och helpdesk samt att genom digitala varningsgruppen fortsätta det brottsförebyggande arbetet.	Polismyndigheten, MCF och Stöldskydds-föreningen	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter Budgetpropositionen 2025
13.6	Polismyndigheten fördjupar fortsatt samarbetet med Europol avseende brottsförebyggande arbete.	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter
13.7	Polismyndigheten deltar fortsatt i Europols Joint Cybercrime Action Taskforce.	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndighetens ordinarie uppgifter
13.8	Polismyndigheten utvecklar sin förmåga att bekämpa cyberbrott.	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndighetens ordinarie uppgifter
13.9	**Ny:** Polismyndigheten har inrättat en permanent nationell cyberinsatsstyrka vid Nationellt IT-brottscentrum.	Polismyndigheten	2026	Pågående arbete inom ramen för myndighetens ordinarie uppgifter
13.10	**Ny:** Regleringen om hemliga och preventiva tvångsmedel ses över inom ramen för en särskild utredning (Utredningen om hemliga och preventiva tvångsmedel, Ju2025:04). Ett deluppdrag tar sikte på att utreda och föreslå en möjlighet att störa och avbryta pågående brott eller brottslig verksamhet i cybermiljö för att förbättra de brottsbekämpande myndigheternas samlade förmåga att ingripa mot sådan brottslighet.	Hemliga och preventiva tvångsmedel – en effektiv och tydlig reglering Dir. 2025:12	2025–2026, uppdraget ska redovisas senast den 29 maj 2026	
13.11	**Ny:** Lagrådsremiss för att genomföra EU:s e-bevisningspaket, SOU 2024:85 Effektivare gränsöverskridande inhämtning av elektroniska bevis.	Regeringen	2025–2026	EU:s förordning om e-bevisning föreslås träda i kraft den 18 augusti 2026

Regeringskansliet
Växel: 08-405 10 00
www.regeringen.se