SVERIGES RIKSDAG

Försvarsutskottets betänkande 2024/25:FöU8

Nationell strategi för cybersäkerhet 2025–2029

Sammanfattning

Utskottet föreslår att riksdagen lägger skrivelsen om en nationell strategi för cybersäkerhet 2025–2029 till handlingarna. I skrivelsen presenteras regeringens inriktning för Sveriges cybersäkerhet med fokus på tre områden, s.k. pelare:

- pelare A: Systematiskt och effektivt cybersäkerhetsarbete
- pelare B: Utvecklad kunskap och kompetensutveckling inom cybersäkerhet
- pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter.

Strategin innehåller mål inom flera områden och en handlingsplan som tar sikte på att bemöta de hot och sårbarheter som identifieras i strategin.

Utskottet föreslår vidare att riksdagen avslår motionsyrkandena.

I betänkandet finns två reservationer (C) och ett särskilt yttrande (S, MP).

Behandlade förslag

Skrivelse 2024/25:121 Nationell strategi för cybersäkerhet 2025–2029.
Två yrkanden i en följdmotion.

Innehållsförteckning

Utskottets förslag till riksdagsbeslut

1. Placeringen av arbetet med Sveriges totala cybersäkerhetsarbete

Riksdagen avslår motion 2024/25:3388 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkande 1.

Reservation 1 (C)

2. Totalsträckskrypterade kommunikationstjänster

Riksdagen avslår motion 2024/25:3388 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkande 2.

Reservation 2 (C)

3. Skrivelsen

Riksdagen lägger skrivelse 2024/25:121 till handlingarna.

Stockholm den 5 juni 2025

På försvarsutskottets vägnar

Peter Hultqvist

Följande ledamöter har deltagit i beslutet: Peter Hultqvist (S), Jörgen Berglund (M), Johan Andersson (S), Hanna Westerén (S), Gulan Avci (L), Erik Ezelius (S), Hanna Gunnarsson (V), Mikael Larsson (C), Lars Püss (M), Emma Berginger (MP), Per Söderlund (SD), Markus Selin (S), Camilla Brunsberg (M), Göran Hargestam (SD), Yusuf Aydin (KD), Oskar Svärd (M) och Carl Nordblom (M).

Redogörelse för ärendet

Ärendet och dess beredning

I betänkandet behandlar utskottet regeringens skrivelse 2024/25:121 Nationell strategi för cybersäkerhet 2025–2029 samt en följdmotion.

En förteckning över de behandlade förslagen finns i bilaga 1. I bilaga 2 finns en handlingsplan som regeringen kopplar till skrivelsen. Handlingsplanen innehåller aktiviteter som svarar mot regeringens inriktning.

Skrivelsens huvudsakliga innehåll

Regeringen har tagit fram en ny nationell strategi för cybersäkerhet. Den beskriver regeringens inriktning för arbetet med frågor av betydelse för Sveriges cybersäkerhet.

Strategin utgår från nationella behov och från NIS 2-direktivet och dess allriskperspektiv för att hantera en bredd av utmaningar. I strategin redogörs för ett antal hot och sårbarheter som påverkar Sveriges cybersäkerhet. Strategin bygger på tre pelare som anger inriktningen för Sveriges cybersäkerhetsarbete:

- pelare A: Systematisk och effektivt cybersäkerhetsarbete
- pelare B: Utvecklad kunskap och kompetensutveckling inom cybersäkerhet
- pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter.

Strategin innehåller dessutom mål som tar sikte på ett antal områden för att åstadkomma förflyttningar under strategins löptid och bemöta de hot och sårbarheter som regeringen har redogjort för i strategin.

Till strategin kopplas en handlingsplan (bilaga 2) med ett antal aktiviteter som svarar mot regeringens inriktning och kraven i NIS 2-direktivet. Handlingsplanen kommer att uppdateras löpande.

Utskottets överväganden

Nationell strategi för cybersäkerhet 2025–2029

Utskottets förslag i korthet

Riksdagen avslår motionsyrkanden om placeringen av arbetet med Sveriges totala cybersäkerhetsarbete och om att den nationella cybersäkerhetsstrategin bör inkludera skrivningar om garanterad tillgång till totalsträckskrypterade kommunikationstjänster. Riksdagen lägger skrivelsen till handlingarna.

Jämför reservation 1 (C) och 2 (C) samt det särskilda yttrandet (S, MP).

Bakgrund och tidigare arbete

Nationell strategi för cybersäkerhet ersätter den tidigare strategin Nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213).

Regeringen inledde under 2023 ett arbete med att utveckla Nationellt cybersäkerhetscenter (NCSC) med målet att centret bl.a. ska utgöra navet i det nationella cybersäkerhetsarbetet. Under 2023 tillsattes en s.k. bokstavsutredning med uppdrag att se över centrets verksamhet (Fö 2023:A). Utifrån den utredningen har regeringen beslutat att NCSC fr.o.m. den 1 november 2024 ska finnas inom Försvarets radioanstalt (FRA) samt att NCSC:s chef ska utses av regeringen. Utredningens övriga förslag bereds inom Regeringskansliet.

I december 2023 behandlade utskottet regeringens skrivelse 2023/24:26 om Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet (bet. 2023/24:FöU2). Utskottet välkomnade åtgärder som syftar till att ytterligare förstärka det nationella cybersäkerhetscentrets verksamhet när det gäller organisering och styrning, bl.a. till förmån för samverkan med näringslivet och utvecklade lägesbilder. Utskottet ansåg att det nationella cybersäkerhetscentret redan då skulle ses som ett mycket viktigt steg framåt, och utskottet såg fram emot att ta del av centrets fortsatta utveckling, t.ex. i fråga om att utreda och dra lärdom av större it-relaterade incidenter, förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter, främja it-incidentrapportering m.m.

I samband med totalförsvarsbeslutet för perioden 2025–2030 behandlade utskottet frågor om cybersäkerhet. (prop. 2024/25:34, bet. 2024/25:FöU2, rskr. 2024/25:114). Utskottet konstaterade att flera åtgärder vidtagits de senaste åren för en förbättrad informations- och cybersäkerhet, i Sverige och inom EU, men att mycket arbete ännu kvarstod. Utskottet välkomnade regeringens breda satsning i budgetpropositionen för 2025 för att stärka informations- och cybersäkerhetsarbetet inklusive åtgärder för att långsiktigt

stödja kompetensutvecklingen på området genom forskning, utbildning och information. Vidare anförde utskottet att det såg fram emot att följa utvecklingen av det ombildade NCSC med FRA som kommande huvudman och att de hade förväntningar om att centret skulle bidra till en starkare nationell struktur och en tydlig knutpunkt för cybersäkerhetsarbetet.

I NIS 2-direktivet[1] fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå i hela EU. Regeringen tillsatte under 2023 en utredning för att bl.a. föreslå de anpassningar av svensk rätt som bör göras till följd av direktivet, och i mars 2024 överlämnade utredningen sitt delbetänkande (SOU 2024:18). Ansvarsförhållandena för de aktörer som omfattas av NIS 2-direktivet kommer att definieras i en nationell reglering som införlivar direktivet i Sverige. Detta lagstiftningsarbete är under beredningen, och regeringen avser att lämna propositionen om en ny cybersäkerhetslag till riksdagen hösten 2025.

I Sverige och inom EU har de senaste årens omfattande teknikutveckling lett till att förslag om lagring av och tillgång till elektronisk information tagits fram. Totalsträckskrypterade tjänster, även kallade end-to-end krypterade tjänster är en central del i aktuella diskussioner inom området. Totalsträcks-krypterade tjänster är sådana tjänster i vilka bara sändare och mottagare av kommunikation kan ta del av informationen, även när informationen överförs genom internetbaserade kommunikationstjänster. I EU har förslaget om att fastställa regler för att förebygga och bekämpa sexuella övergrepp mot barn förhandlats sedan det lades fram 2022. Förslaget innebär ökade befogenheter för nationella myndigheter att upptäcka och utreda misstänka sexuella övergrepp och kontakt med barn (gromning) som sker på kommunikations-tjänster på internet.

I augusti 2021 gav regeringen en särskild utredare i uppdrag att analysera och utvärdera den nuvarande regleringen om lagring av och tillgång till uppgifter om elektronisk kommunikation för brottsbekämpande syften. Syftet med uppdraget var att säkerställa att de brottsbekämpande myndigheternas tillgång till information förbättras och inte försämras över tid på grund av teknikutveckling och förändrade kommunikationsvanor, samtidigt som respekten för mänskliga rättigheter säkerställs. I maj 2023 redovisades utredningens slutsatser i betänkandet Datalagring och åtkomst till elektronisk information (SOU 2023:22). I utredningen föreslås bl.a. nya lagar och ändringar i lagstiftning kopplad till brottsbekämpande myndigheters tillgång till elektronisk information. Lagändringarna föreslås träda i kraft den 1 mars 2026. Utredningen har remitterats till berörda myndigheter och aktörer och förslagen bereds vidare inom Regeringskansliet.

[1] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

Skrivelsen

Strategins utgångspunkter

Regeringen anför att den nationella cybersäkerhetsstrategin utgår från nationella behov och från NIS 2-direktivet och dess allriskperspektiv för att hantera en bredd av utmaningar. Mot bakgrund av det säkerhetspolitiska läget fokuserar strategin därtill särskilt på antagonistiska hot i hela hotskalan.

I skrivelsen konstaterar regeringen att cyberförsvar är en integrerad del av det militära försvaret och bidrar till Sveriges samlade förmåga att möta ett väpnat angrepp. Cyberoperationer är en lika självklar del av krigföringen som mark, sjö-, luft- och rymdoperationer. I fredstid kan Försvarsmaktens cyberförsvarsresurser användas för att stödja samhället under kriser eller andra allvarliga händelser. Regeringen lyfter även fram att ansvarsprincipen, dvs att den som i normala fall ansvarar för en verksamhet, också har detta ansvar under en krissituation.

Strategins primära målgrupp är myndigheter med särskilt ansvar för verksamhet som bedrivs inom ramen för NCSC, tillsynsmyndigheter inom den samlade cybersäkerhetsregleringen samt andra organisationer som ingår i beredskaps- och NIS 2-sektorerna. Regeringen betonar dock att strategin och den tillhörande handlingsplanen ska vara till nytta för hela samhället.

Internationell kontext för nationell cybersäkerhet

Sveriges cybersäkerhet och reglering på området styrs delvis nationellt men också i ökande grad av den internationella kontexten. På lagstiftningsområdet styrs utvecklingen främst av EU-samarbetet. EU-kommissionen har tagit flera initiativ till reglering och normgivning inom cybersäkerhet och digitala frågor, inte minst cyberresiliensförordningen[2] och cybersäkerhetsakten[3], vilka båda är direkt tillämpliga i EU:s medlemsstater. Därtill har Nato ett växande fokus på strategiska cybersäkerhets- och teknikfrågor, och inom Nato bedrivs ett omfattande arbete med cyberförsvar och strategiska tekniker.

Cybersäkerhetslandskapet

I cybersäkerhetsstrategin redogör regeringen för olika typer av hot och sårbarheter som kan påverka samhällsviktig verksamhet och ytterst Sveriges säkerhet. När det gäller cyberhotaktörer lyfter regeringen fram hot från statliga aktörer, hot från cyberaktivister och hot från cyberbrottslighet och kriminella grupperingar. Sårbarheter i cybersäkerhetslandskapet kan bl.a. röra organisatoriska, tekniska, infrastrukturella och mänskliga faktorer. Strategin lyfter

[2] Europaparlamentets och rådets förordning (EU) 2024/2847 av den 23 oktober 2024 om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordningarna (EU) nr 168/2013 och (EU) 2019/1020 och direktiv (EU) 2020/1828 (cyberresiliensförordningen).
[3] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

exempelvis fram brister i cybersäkerhetsarbetet, komplex reglering, kompetens och kunskap, bristande incidenthantering samt sårbara leveranskedjor, beroenden och produkter.

Regeringens inriktning

Den nationella cybersäkerhetsstrategin utgår från tre pelare som anger riktningen för Sveriges cybersäkerhetsarbete:

- pelare A: Systematiskt och effektivt cybersäkerhetsarbete
- pelare B: Utvecklad kunskap och kompetensutveckling inom cybersäkerhet
- pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter.

Varje pelare innehåller ett antal mål med tillhörande resultatindikatorer. Strategin sträcker sig t.o.m. 2029, och i skrivelsen redogör regeringen även för ”önskat läge 2030” som speglar regeringens vision för var Sverige befinner sig och vilka förflyttningar som skett, inom respektive mål vid strategins utgång. Givet det långsiktiga utvecklingsarbetet med NCSC, där centret ska vara navet för det nationella cybersäkerhetsarbetet, ser regeringen att centret har en väsentlig roll inom ett flertal av målområdena och uppföljningen av dessa.

Regeringen presenterar även en handlingsplan (bilaga 2) som innehåller aktiviteter som svarar mot regeringens inriktning och kraven i NIS 2-direktivet Handlingsplanens innehåll kommer att uppdateras löpande och aktiviteter tillföras för att stegvis uppnå målen.

Pelare A: Systematiskt och effektivt cybersäkerjetsarbete

Syftet med pelare A är att öka svensk motståndskraft genom att ge förutsättningar för alla samhällets organisationer att stärka sitt systematiska cybersäkerhetsarbete, att öka säkerheten i digitala leveranskedjor och produkter, och om att skydda kritiska system och verksamheter.

Regeringen anger följande mål för arbetet med pelare A:

- Ökat cybersäkerhetsarbete hos privata och offentliga organisationer
- Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering
- Stärkt cybersäkerhetsarbete inom kritisk infrastruktur
- Robustare digitala leveranskedjor och minskat beroende
- Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete
- Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete

Övergripande resultatindikatorer för målen i pelare A är att

- antalet organisationer som nyttjat NCSC:s råd och stöd inom cybersäkerhetsområdet har ökat

- antalet statliga myndigheter som genomfört cybersäkerhetsmätningar har ökat
- andelen organisationer som genom systematiska arbetssätt implementerat cybersäkerhetsåtgärder, både administrativa och tekniska, har ökat.

Pelare B: Utvecklad kunskap och kompetens inom cybersäkerhet

Pelare B handlar om att öka medvetenheten, utveckla och bygga kompetens inom cybersäkerhet på alla nivåer samt främja svensk forskning, innovation och säker tillämpning av ny teknik.

Regeringen anger följande mål för arbetet med pelare B:

- Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället
- Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet
- Stärkt forskning och innovation på cybersäkerhetsområdet
- Stärkt förmåga att hantera framväxande teknologiers risker och möjligheter.

Övergripande resultatindikatorer för målen i pelare B är att

- andelen personer som har nåtts, och tagit till sig av, informationskampanjer om cybersäkerhet har ökat
- antalet forsknings- och innovationsprojekt inom cybersäkerhet som har fått EU-finansiering har ökat
- antalet företag verksamma inom cybersäkerhet i Sverige har ökat.
- antalet utbildade inom cybersäkerhet eller motsvarande har ökat
- antalet företag som genomgått verksamhetscertifiering inom cybersäkerhet har ökat.

Pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter

Pelare C syftar till att stärka förmågan att snabbt identifiera hot och förebygga cybersäkerhetsincidenter genom god informationsdelning samt att stärka det nationella systemet för och samarbetet kring incidenthantering. Hantering av cybersäkerhetsincidenter handlar om att identifiera, svara på och hämta sig från incidenter genom att vara väl förberedd, förstå vad som har hänt och utvärdera om agerandet varit adekvat. Vid cybersäkerhetsincidenter som drabbat flera länder är internationellt samarbete avgörande för en effektiv incidenthantering.

Regeringen anger följande mål för arbetet med pelare C:

- Effektivare och säkrare informationsdelning nationellt och internationellt
- Stärkt privat-offentlig hantering av cybersäkerhetsincidenter
- Utvecklad förmåga att förebygga och bekämpa cyberbrott.

Övergripande resultatindikatorer för målen i pelare C är att

- andelen organisationer med kvalificerade processer för hantering av cybersäkerhetsincidenter har ökat
- processer hos berörda statliga myndigheter för att rapportera in incidenter har effektiviserats
- antalet cybersäkerhetsincidenter som rapporterats in har ökat
- informationsdelning om incidenter har ökat mellan berörda myndigheter
- återkopplingen från statliga myndigheter som tar emot incident-rapportering till organisationer som rapporterar incidenter har förbättrats.

Genomförande och uppföljning

Den nationella strategin för cybersäkerhet kommer enligt skrivelsen att uppdateras regelbundet och minst vart femte år utvärderas på grundval av strategins resultatindikatorer och i enlighet med NIS 2-direktivets krav. Strategin ska omsättas i konkret handling bl.a. genom specifika uppdrag och styrning. En redogörelse för detta finns i handlingsplanen i bilaga 2.

Motionen

I kommittémotion 2024/25:3388 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkande 1 uttrycker motionärerna oro över att arbetet med Sveriges totala cybersäkerhetsarbete placerats hos FRA. Motionärerna anför att FRA saknar erfarenhet av arbete med aktörer brett i samhället och att detta begränsar myndighetens möjlighet att ansvara för ökad transparens och tillitsfullt samarbete mellan aktörer inom alla delar av samhället.

Vidare anser motionärerna i yrkande 2 att Sveriges strategi för cybersäkerhet bör inkludera skrivningar om garanterad tillgång till totalsträckskrypterade kommunikationstjänster.

Utskottets ställningstagande

Utskottet anser att det är angeläget att se över och uppdatera arbetet med cybersäkerhet och lagstiftningen kring cybersäkerhet i takt med den snabba och omfattande tekniska utvecklingen inom området. Utskottet välkomnar därför den nya nationella strategin för cybersäkerhet och ser fram emot den kommande beredningen av de lagförslag inom cybersäkerhetsområdet som regeringen avser att presentera i en proposition under hösten 2025.

Utskottet ser positivt på att *en* aktör har det övergripande ansvaret och utgör navet för det samlade nationella cybersäkerhetsarbetet. I enlighet med vad utskottet tidigare anfört välkomnar det åtgärder som syftar till att ytterligare förstärka NCSC:s verksamhet när det gäller organisering och styrning, bl.a. till förmån för samverkan med näringslivet och utvecklade lägesbilder. Utskottet vidhåller sin bedömning att NCSC innebär ett viktigt steg framåt, och utskottet avser att följa centrets fortsatta utveckling, inte minst i fråga om att utreda och

dra lärdom av större it-relaterade incidenter, förebygga, upptäcka och hantera cyberangrepp och andra it-incidenter samt främja it-incidentrapportering. Utskottet konstaterar att omfattande förändringar har gjorts av hur samhällets cybersäkerhetsarbete organiseras och styrs, och frågan är även under fortsatt beredning. Utskottet ser inget behov av att se över eller ompröva placeringen av NCSC hos FRA i enlighet med vad som anförs i motion 2024/25:3388 (C) yrkande 1. Motionsyrkandet avstyrks.

När det gäller totalsträckskrypterade kommunikationstjänster konstaterar utskottet att en reglering av sådana tjänster förhandlas inom EU och bereds inom Regeringskansliet. Utskottet ser inte skäl att föregripa det pågående arbetet och bedömer därför att det i nuläget inte är aktuellt med skrivningar om garanterad tillgång till totalsträckskrypterade kommunikationstjänster i den nationella cybersäkerhetsstrategin. Utskottet avstyrker således motion 2024/25:3388 (C) yrkande 2.

Avslutningsvis föreslår utskottet att riksdagen lägger skrivelsen till handlingarna.

Reservationer

1. Placeringen av arbetet med Sveriges totala cybersäkerhetsarbete, punkt 1 (C)

av Mikael Larsson (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 1 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion 2024/25:3388 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkande 1.

Ställningstagande

Cybersäkerhetsfrågorna blir alltmer angelägna såväl i ljuset av det bekymrande omvärldsläget som mot bakgrund av teknikutvecklingen. Regeringens probleminsikt är god och skrivelsen angriper många av Sveriges utmaningar inom cybersäkerhet. Jag vill dock uttrycka oro över placeringen av arbetet med Sveriges totala cybersäkerhetsarbete hos Försvarets radioanstalt (FRA). FRA är utan tvekan ytterst kompetent inom cyberförsvar, men saknar fullständigt erfarenhet av arbete med aktörer brett i samhället.

Adekvata arbetssätt för incident- och kontinuitetshantering saknas hos många organisationer och få övar dessa förmågor. Bristande incidenthantering utgör en allvarlig risk för organisationer. Informationsdelning och samarbete mellan och inom den privata och den offentliga sektorn kräver bl.a. uppbyggda kommunikationsvägar och adekvata processer samt tillit aktörer emellan. Dessa processer behöver bl.a. utgå från och ta hänsyn till privata aktörers affärsintressen och sekretess för affärs- och driftsförhållanden. Outvecklat och bristande samarbete mellan det privata och det offentliga, nationellt såväl som internationellt, utgör en sårbarhet. Flera andra länder har gjort liknande försök med att ge uppdraget för den breda cybersäkerheten till landets mest hemlighetsfulla organisationer. Efter ett tag har det konstaterats att det finns kulturhinder i dessa organisationer för att ha ett tillräckligt öppet och inkluderande arbete, och uppdraget har därefter flyttats över till andra organisationer. Det är fortfarande mycket oklart hur FRA i praktiken ska säkra att antalet cybersäkerhetsincidenter som rapporteras in ökar eller att informationsdelning om incidenter ökar mellan de myndigheter som är berörda.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

2. Totalsträckskrypterade kommunikationstjänster, punkt 2 (C)

av Mikael Larsson (C).

Förslag till riksdagsbeslut

Jag anser att förslaget till riksdagsbeslut under punkt 2 borde ha följande lydelse:

Riksdagen ställer sig bakom det som anförs i reservationen och tillkännager detta för regeringen.

Därmed bifaller riksdagen motion 2024/25:3388 av Mikael Larsson och Niels Paarup-Petersen (båda C) yrkande 2.

Ställningstagande

Cybersäkerhetsstrategin bör inkludera skrivningar om garanterad tillgång till totalsträckskrypterade kommunikationstjänster. Mål 7 i den nationella cybersäkerhetsstrategin är Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället. Cyberhygien inkluderar enligt NCSC totalsträckskrypterade tjänster. Men regeringen vill stoppa dessa, trots att Försvarsmakten själv i en instruktion meddelar att all information till och från försvaret ska ske via sådana tjänster när det inte är tal om säkerhetsskyddsklassificerade uppgifter.

För att kunna skydda sin information är det avgörande att kunna dela information utan att den delas till andra än den önskade mottagaren. Jag ser skäl till oro när det gäller behoven av tillförlitlig och säker digital infrastruktur och med tanke på att digitala tjänster växer i betydelse och omfattning. Små och medelstora företags motståndskraft och skydd av affärshemligheter är en väsentlig del när det gäller att slå vakt om Sveriges samlade konkurrens- och motståndskraft, men företagens möjlighet att kommunicera i säkerhet utan risk för att bli spionerade på av en tredje part ska, enligt regeringen, alltså inte längre vara tillgänglig eftersom totalsträckskrypterade tjänster ska förbjudas om de inte installerar bakdörrar.

Riksdagen bör ställa sig bakom det som anförs i reservationen och tillkännage detta för regeringen.

Särskilt yttrande

Skrivelsen, punkt 3 (S, MP)

Peter Hultqvist (S), Johan Andersson (S), Hanna Westerén (S), Erik Ezelius (S), Emma Berginger (MP) och Markus Selin (S) anför:

Omfattande satsningar behöver göras på svensk cybersäkerhet. Vi välkomnar en ambitionshöjning inom området och vill i sammanhanget lyfta fram några aspekter som är viktiga för oss i det pågående och kommande arbetet med att stärka den svenska cybersäkerheten. Den dåvarande socialdemokratiskt och miljöpartistiskt ledda regeringen överlämnade Sveriges första nationella strategi för samhällets informations- och cybersäkerhet till riksdagen den 22 juni 2017 (skr. 2016/17:213). Strategin uttryckte regeringens övergripande prioriteringar och utgjorde en plattform för Sveriges fortsatta utvecklingsarbete inom området. Strategin skulle ge långsiktighet och effektivitet i arbetet samt höja medvetenheten och kunskapen i hela samhället, och 2017 års strategi hade sex huvudområden. För var och en av dåvarande sex prioriteringar ställde regeringen upp ett antal målsättningar och inriktningar för hur målsättningarna ska nås.

I den rådande cybermiljön ser vi stora risker eftersom antagonister går ifrån att störa till att förstöra. Teknikutvecklingen går snabbt, och världsläget är osäkert, och Socialdemokraterna och Miljöpartiet förstår att strategier och arbetssätt emellanåt kan behöva uppdateras. Men vi ser med tvekan på den sverigedemokratiskt stödda regeringens uppdaterade strategi för cybersäkerhet: Nationell strategi för cybersäkerhet 2025–2029. Sex områden har i den uppdaterade strategin blivit tre, i sak även snarlika. Den nuvarande regeringen har dessutom skapat ytterligare kompletterande strategier, inklusive Sveriges första försvars- och säkerhetsstrategi för rymden, Nationell säkerhetsstrategi, Sveriges utrikes- och säkerhetspolitik inom cyberfrågor och digitala frågor, och snart kommer även en digitaliseringsstrategi. Vi är tveksamma till att ett staplande av olika strategier gör helheten mer strategisk och långsiktig för arbetet med informations- och cybersäkerhet. Härtill ser vi en tilltagande otydlighet kring ansvarsfördelningen som råder bland olika statsråd och departement när det gäller digitalisering och cyberpolitiken. Det är högst tveksamt om styrningen av området är samlad och säkerställd i Regeringskansliet. Det finns risker kring ansvarsfördelning, kompetens och effektiva former för samordning av informations- och cybersäkerhetsfrågorna. Just det senaste varnade även Riksrevisionen för redan den 27 april 2023 i sin rapport Regeringens styrning av samhällets informations- och cybersäkerhet − både brådskande och viktig.

Med den senaste uppdaterade strategin följer även bilaga 2, Organisationer med roller och ansvarsområden inom cybersäkerhet, som innehåller klargöranden kring organisationer, vilket kan bidra med substans. Men, vi ställer oss undrande kring bilaga 1, Handlingsplan, samt avsnittet Översikt

över utmaningar och mål, som till stora delar beskriver kontinuerliga processer och önskade tillstånd som våra myndigheter förväntas hantera mer grundläggande och löpande. Här kan även nämnas att Socialdemokraterna den 4 oktober 2024 framförde fler förslag kring cyberpolitiken i motion 2024/25:3023 Försvar och samhällets krisberedskap av Peter Hultqvist m.fl. (S) samt att Miljöpartiet har framfört förslag kring cyberpolitiken i motion 2024/25:3038 Stärkt beredskap och ett robustare samhälle av Daniel Helldén m.fl. (MP).

Det svenska cyberförsvaret och beredskapen för cyberangrepp måste stärkas. Det är i dag viktigare än någonsin tidigare att såväl myndigheter som kommuner och företag bedriver ett systematiskt informationssäkerhetsarbete. Det är av särskild vikt att stärka it- och cybersäkerheten samt samhällets förmåga att möta asymmetriska cyberhot. Den nationella cyberkompetensen behöver stärkas för att kunna bemöta cyberangrepp och antagonistiska cyberhot. Regeringen bör ta initiativ till kunskapsuppbyggnad inom cybersäkerhetsområdet inom den offentliga sektorn.

Angreppen från cyberkriminella blir allt vanligare samtidigt som vi ser att angreppen även ökar från främmande stater. Främmande stater har resurser att skada samhällsviktiga funktioner såsom livsmedelsförsörjning, elförsörjning och sjukvård med långvariga samhällsstörningar som följd. Statens ansvar för cybersäkerheten måste därför stärkas. Cyber- och informationssäkerheten är en verksamhet med en egen karaktär och prägel. Kungliga Ingenjörsvetenskapsakademin har i sin rapport Cybersäkerhet för ökad konkurrenskraft föreslagit att en haverikommission ska upprättas för cyberincidenter. Kommissionen skulle enligt förslaget få i uppdrag att utreda, diskutera och analysera cyberincidenter och redovisa rekommendationer och lärdomar från dessa. Sammantaget avser vi att noga följa regeringens fortsatta arbete med frågorna och återkomma med konkreta förslag till riksdagen i andra sammanhang.

BILAGA 1

Förteckning över behandlade förslag

Skrivelsen

Regeringens skrivelse 2024/25:121 Nationell strategi för cybersäkerhet 2025–2029.

Följdmotionen

2024/25:3388 av Mikael Larsson och Niels Paarup-Petersen (båda C):

1. Riksdagen ställer sig bakom det som anförs i motionen om lämpligheten i placeringen av arbetet med Sveriges totala cybersäkerhetsarbete hos Försvarets radioanstalt och tillkännager detta för regeringen.
2. Riksdagen ställer sig bakom det som anförs i motionen om att cybersäkerhetsstrategin bör inkludera skrivningar om att tillgång till totalsträckskrypterade kommunikationstjänster ska garanteras och tillkännager detta för regeringen.

BILAGA 2

Regeringens handlingsplan 2025

Handlingsplan 2025				
Mål/aktivitetsnr.	**Beskrivning**	**Ansvarig(a) utförare för aktiviteten***	**Tidsperiod**	**Relevant(a) styrmedel**
Pelare A mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer				
1:1	**Nationellt cybersäkerhetscenter (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	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
1:2	**CER- och NIS 2-direktiven genomförs nationellt på ett harmoniserat sätt.** Syfte: Genom att, bland annat med stöd i slutsatserna och förslagen i betänkandena om genomförande av NIS 2- och CER-direktiven (SOU 2024:18 och 2024:64), stärka och harmonisera lagstiftningen på området skapas förutsättningar för att cybersäkerhetsarbetet hos organisationer ska få större genomslag samt bidra till ökad motståndskraft i samhällsviktig verksamhet och därmed ett stärkt civilt försvar.	Regeringen	2025	Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet)

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

				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	**En särskild utredare ska analysera behovet av och föreslå åtgärder och kompletterande författningsbestämmelser som behövs i syfte att anpassa svensk rätt till EU:s cyberresiliensförordning (CRA).** Syfte: Att bland annat analysera vilka svenska regelverk som berörs, föreslå sanktionsbestämmelser samt vilken eller vilka myndigheter som bör bli nationell marknadskontrollmyndighet och anmälande myndighet.	Fi 2024:07	2025	Dir 2024:119
1:4	**Myndigheten för samhällsskydd och beredskap (MSB) säkerställer att utbildningar kommer till stånd för organisationer som omfattas av NIS 2-direktivet och beredskapssektorerna.**	MSB	2024–2027	Budgetpropositionen 2025

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	Syfte: Aktiviteten stödjer målet genom att höja kompetensen hos organisationer som ska bedriva ett systematiskt cybersäkerhetsarbete.			
1:5	**FRA och MSB 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, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver.** Syfte: Aktiviteten stödjer målet genom att främja moderna cyberriskhanteringsåtgärder som en del i organisationers cybersäkerhetsarbete.	FRA och MSB 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)
1:6	**MSB fortsätter utveckla och förvalta råd och stöd för organisationers systematiska cybersäkerhetsarbete.** Syfte: Aktiviteten stödjer målet genom att organisationer kan få vägledning i sitt cybersäkerhetsarbete.	MSB	Tills vidare	Förordning med instruktion för MSB
1:7	**MSB fortsätter arbetet med analyser och temarapporter inom cybersäkerhetsområdet.**	MSB	Tills vidare	Förordning med instruktion för MSB EU-finansierat projekt ENIAC

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	Syfte: Myndighetens arbete med analyser och temarapporter är till gagn för organisationers cybersäkerhetsarbete och arbetet med att stärka samhällets motståndskraft.			
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	Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA)
1:9	**MSB vidareutvecklar Cybersäkerhetskollen för att kunna bistå fler organisationer i fler processer och kunna förmedla en fördjupad nationell lägesbild kring cybersäkerhetsnivån i samhällsviktiga verksamheter.**	MSB	2025–2027	Budgetpropositionen 2025

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	Syfte: Genom att utöka Cybersäkerhetskollen med stöd för bedömning av organisationens it- och OT-säkerhet samt leveranskedjor får organisationer ett ändamålsenligt verktyg att både bedöma sin nivå inom flera centrala områden samt 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.			
Pelare A mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering				
2:1	**MSB tillförs medel för förberedelse av en nationell kartläggning av kommuners tekniska cybersäkerhetsförmåga.** Syfte: Förbereda en nationell kartläggning av små och medelstora aktörer för att få en överblick över den tekniska cybersäkerhetsförmågan hos målgruppen.	MSB	2025–2027	Budgetpropositionen 2025
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	Berörda statliga myndigheter	2025–2026	Regleringsbrev

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	inom informations- och cybersäkerhet och ger regeringen underlag för ytterligare åtgärder på området.			
2:3	**MSB 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.	MSB	2025–2027	Budgetpropositionen 2025
2:4	**FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att inkludera och specificera cybersäkerhetsrelaterade krav för IKT-produkter och IKT-tjänster vid offentlig upphandling, inbegripet vad gäller cybersäkerhetscertifiering, kryptering och användning av cybersäkerhetsprodukter med öppen källkod, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta.** Syfte: Att erbjuda vägledning avseende säkrare upphandling vilket är av särskild vikt för att höja cybersäkerheten i statlig och kommunal förvaltning.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

2:5	**Regeringskansliet uppdaterar strategins bilaga 2, ”Organisationer med roller och ansvarsområden inom cybersäkerhet”, när NIS 2-regleringen implementerats nationellt och definierat ansvarsförhållanden samt när uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (dir. 2024:111) redovisats och förslagen omhändertagits.** Syfte: Aktiviteten stödjer målet genom att Regeringskansliet klargör hur ansvaret för det nationella cybersäkerhetsarbetet är fördelat.	Regeringskansliet	2025	NIS 2-direktivet
2:6	**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	Dir. 2024:111

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

Pelare A mål 3: Stärkt säkerhetsarbete inom kritisk infrastruktur				
3:1	**MSB tillhandahåller stöd för samhällsviktig verksamhets arbete med säkerhet i operativ teknik (OT).** Syfte: Aktiviteten stödjer målet genom att erbjuda operatörer stöd kring säkerhet i de OT-system som kritisk infrastruktur ofta är beroende av.	MSB	Tills vidare	Förordning med instruktion för MSB
3:2	**FRA och MSB ska inom ramen för NCSC att 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, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta.** Syfte: Aktiviteten stödjer målet genom anpassade riktlinjer avseende säker och tillgänglig konnektivitet, vilket samhället är beroende av.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)
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

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	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.			om digital operativ motståndskraft för finanssektorn Lag (2024:1278) med kompletterande bestämmelser till EU:s förordning om digital operativ motståndskraft för finanssektorn
Pelare A mål 4: Robustare digitala leveranskedjor och minskat beroende				
4:1	**Berörda statliga myndigheter fortsätter inom ramen för etablerad NCSC-samordning kring standardisering av cybersäkerhet.** Syfte: Att genom myndighetsgemensam samordning samverka frågor av myndighetsöverskridande relevans kring internationell standardisering på cybersäkerhetsområdet.	PTS och FMV i samverkan med Försvarsmakten, FRA, MSB Säkerhetspolisen och Polismyndigheten	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**	FMV	Tills vidare	Lagen (2021:553) med kompletterande

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	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 och relevanta processer.			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	**MSB 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	MSB	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:5 (Fö2025/00390)

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	förvaltningen som regeringen den 19 september 2019 uppdrog MSB att upprätta (Ju2019/03058/SSK och Ju2019/02421/SSK).			
4:4	**FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för cybersäkerhet i leveranskedjan för IKT-produkter och IKT-tjänster som används av entiteter när de tillhandahåller sina tjänster, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta.** Syfte: Aktiviteten stödjer målet genom att bidra till organisationers möjlighet att säkra sina leveranskedjor och därmed minska sin sårbarhet för cyberangrepp och störningar.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)
Pelare A mål 5: Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete				
5:1	**MSB är nationell gemensam kontaktpunkt i enlighet med NIS-direktivet.** Syfte: Aktiviteten stödjer målet genom att MSB i egenskap av kontaktpunkt bland annat bedriver tillsynssamordning via ett samarbetsforum för effektiv och likvärdig tillsyn kopplat till NIS-regleringen samt deltar i internationell samverkan rörande regulatoriska policyfrågor	MSB	2025	Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	(Sveriges representant i NIS-Cooperation Group).			
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.	FRA, Försvarsmakten, MSB, Säkerhetspolisen, 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.** Syfte: Aktiviteten stödjer målet genom att skapa bättre förutsättningar för tillsynsmyndigheter att hantera de ökade kraven rörande tillsyn som följer av NIS 2-direktivet. Genom aktiviteten ges tillsynsverksamheten under NIS 2-direktivet goda förutsättningar från dag ett.	Vissa länsstyrelser, Läkemedelsverket, Inspektionen för vård och omsorg, Transportstyrelsen, Livsmedelsverket, Statens energimyndighet samt PTS	2025–2027	Budgetpropositionen 2025

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

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	Förordningar med myndigheternas instruktioner Säkerhetsskyddslag (2018:585) Säkerhetsskydds-förordning (2021:955)
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	Förordningar med myndigheternas instruktioner Säkerhetsskyddslag (2018:585) Säkerhetsskydds-förordning (2021:955)
5:6	**MSB förvaltar, utvecklar och tillhandahåller publik databas över svensk terminologi inom cybersäkerhetsområdet.** Syfte: Att säkerställa en ensad terminologi som förenklar organisationers cybersäkerhetsarbete och samarbete sinsemellan.	MSB	Tills vidare	Förordning med instruktion för MSB

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

5:7	**MSB 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.	MSB	2025–2027	Förordning med instruktion för MSB Budgetpropositionen 2025
Pelare A mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete				
6:1	**FRA och MSB 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, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta.** Syfte: Aktiviteten stödjer målet genom att ta fram riktlinjer som kan vara till gagn för små och medelstora företag som utvecklar sitt cybersäkerhetsarbete.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)
6:2	**Medel tillförs MSB för att intensifiera det brottsförebyggande samarbetet med Stöldskyddsföreningen.**	MSB	2025–2027	Budgetpropositionen 2025

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	Syfte: Genom att vidareutveckla arbetet med målgruppsanpassat stöd förstärks stödet till små och medelstora företag ytterligare.			
Pelare B mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien hos allmänheten				
7:1	**Medel tillförs MSB för att vidareutveckla kampanjen ”Tänk säkert”.** Syfte: Aktiviteten stödjer målet genom att kampanjen syftar till att öka cybersäkerhetsmedvetenheten i samhället vilket långsiktigt bidrar till att höja lägstanivån och därmed motståndskraften mot såväl cyberattacker som andra hybridaktiviteter.	MSB	2025–2027	Budgetpropositionen 2025
Pelare B 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 Kungl. 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**	Försvarsmakten, Säkerhetspolisen samt Försvarshögskolan	Tills vidare	Pågående arbete inom ramen för myndigheternas ordinarie uppgifter

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	kompetensförsörjning inom primärt säkerhetsskyddsområdet. Syfte: Aktiviteten stödjer målet genom ett stärkt samarbete mellan aktörer som syftar till att avhjälpa brister i kompetensförsörjning på säkerhetsområdet			
8:3	**MSB 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.	MSB	Tills vidare	Förordning med instruktion för MSB
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	Mediemyndigheten	Tills vidare	Förordning med instruktion för Mediemyndigheten

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	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.			
8:5	**FRA och MSB 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, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) anger att medlemsstaterna ska anta.** Syfte: Aktiviteten stödjer målet genom att riktlinjer upprättas som bland annat berör	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	centrala frågor för att främja ökad cybersäkerhetskompetens.			
Pelare B mål 9: Stärkt forskning och innovation på cybersäkerhetsområdet				
9:1	**MSB 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.	MSB	Tills vidare	Förordning med instruktion för MSB 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 samordnings-centrum
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.	MSB	2025–2027	Budgetpropositionen 2025

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

9:3	**Medel tillförs för MSB:s vidareutveckling av Cybernoden.** Syfte: Aktiviteten stödjer målet genom att den svenska Cybernodens arbete med att samla näringsliv, akademi och offentlig sektor utvecklas.	MSB	2025–2027	Budgetpropositionen 2025
9:4	**MSB beställer, kvalitetssäkrar och förmedlar forskning och utvecklingsarbete för informations- och cybersäkerhet.** Syfte: Aktiviteten stödjer målet genom att MSB, inom ramen för myndighetens utlysningar inom samhällsskydd och beredskap, också främjar forskning på cybersäkerhetsområdet.	MSB	Tills vidare	Förordning med instruktion för MSB
9:5	**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	2025	Forskning, frihet, framtid – kunskap och innovation för Sverige (prop. 2020/21:60) Myndighetens regleringsbrev
Pelare B mål 10: Stärkt förmåga att hantera framväxande teknologiers risker och möjligheter				
10:1	**Uppdrag till Mediemyndigheten att genomföra en nationell satsning för stärkt**	Mediemyndigheten	2024–2025	Regeringsuppdrag den 14 mars 2024 (Ku2024/00419)

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	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.			
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	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**	Försvarsmakten med stöd av FRA	Tills vidare	Uppgiften som kryptogodkännande myndighet (NCSA/CAA) Förordning med instruktion för Försvarsmakten

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	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.			
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	Uppgiften som kryptogodkännande myndighet (NCSA/CAA) Förordning med instruktion för Försvarsmakten
Pelare C mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt				
11:1	**FRA ska inom ramen för NCSC främja samverkan med privata och offentliga aktörer.** Syfte: Stärkt privat-offentlig samverkan skapar förutsättningar för bland annat effektivare informationsdelning.	FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

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.	FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
11:3	**FRA och MSB ska inom ramen för NCSC 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, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver.** Syfte: Riktlinjer rörande frivilligt informationsutbyte om cybersäkerhet bidrar till effektiv informationsdelning.	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)
11:4	**FRA och MSB 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**	FRA och MSB med bistånd av FMV, Försvarsmakten, Polismyndigheten, PTS och Säkerhetspolisen	2025–2026	Regeringsuppdrag den 27 februari 2025 Fö nr II:4 (Fö2025/00389)

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	12.1, som en del i att fastställa de riktlinjer som direktivets artikel 7.2 a) - j) kräver. Syfte: Aktiviteten stödjer målet genom att adressera delning av information om sårbarheter, vilket utgör en viktig aspekt av effektiv informationsdelning.			
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, MSB, Säkerhetspolisen, Polismyndigheten, FMV och PTS	Tills vidare	Förordningar med myndigheternas instruktioner
Pelare C mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter				
12:1	**FRA fortsätter erbjuda tekniskt detekterings- och varningssystem (TDV) till de mest skyddsvärda verksamheterna.** Syfte: Genom att utveckla och tillhandahålla TDV stärks de mest skyddsvärda verksamheternas förmåga att förebygga och upptäcka cybersäkerhetsincidenter.	FRA	Tills vidare	Förordning med instruktion för FRA

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

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.	MSB i samverkan med berörda aktörer	Tills vidare	Förordning med instruktion för MSB
12:3	**Statliga myndigheter genomför inom ramen för NCSC nationella cybersäkerhetsövningar.** 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.	FRA i samverkan med FMV, Försvarsmakten, MSB, Polismyndigheten, PTS och Säkerhetspolisen	Tills vidare	Förordning om det nationella cybersäkerhetscentret vid Försvarets radioanstalt
12:4	**MSB fortsätter att planera, genomföra, utvärdera cybersäkerhetsövningar, inklusive att utveckla nationell Cyber Range.**	MSB	Tills vidare	Förordning med instruktion för MSB

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	Syfte: Genom att stärka det kollektiva lärandet höjs privata och offentliga organisationers incidenthanteringsförmåga.			
12:5	**MSB skapar en samlad portal med smarta formulär för rapportering av incidenter, tillbud, sårbarheter och cyberhot under olika regelverk, primärt NIS 2- och CER-direktivet.** Syfte: Att förenkla organisationers cybersäkerhetsincidenthanteringsarbete genom att - undanröja krav på duplicerad NIS 2- och CER-rapportering - införa möjlighet till ökat informationsutbyte och ytterligare funktionalitet för både rapporterande och mottagande organisationer. Genom framtida planerad utveckling av portalen väntas också förbättrade möjligheter till informationsdelning och samverkan mellan mottagande statliga myndigheter och andra statliga myndigheter som ytterligare leder till att stärka det nationella incidenthanteringsarbetet.	MSB	Tills vidare	EU-finansierat projekt ENIAC

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

12:6	**MSB 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.	MSB	Tills vidare	Förordning med instruktion för MSB
12:7	**FRA och MSB ska inom ramen för NCSC ta fram riktlinjer för att främja ett aktivt cyberskydd, som en del i att fastställa de riktlinjer som NIS 2-direktivets artikel 7.2 a) - j) kräver.** Syfte: Aktiviteten stödjer målet genom att främja ett aktivt cyberskydd, vilket organisationer kan använda för att stärka sin förmåga att hantera och bemöta cybersäkerhetsincidenter.	FRA och MSB 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

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	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.			
12:9	**Inom ramen för NTSG:s 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	Proposition 2023/24:60 En telesamverkansgrupp för fredstida kriser och höjd beredskap
12:10	**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	Regeringsuppdrag den 27 februari 2025 Fö nr II:2 (Fö2025/00388)

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

12:11	**MSB 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.** Syfte: Att utse behörig myndighet med ansvar för vissa uppgifter enligt NIS 2-direktivet.	MSB	2025	Regeringsuppdrag den 27 februari 2025 Fö nr II:1 (Fö2025/00387)
12:12	**Medel tillförs MSB 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.	MSB	2025–2027	Budgetpropositionen 2025
12:13	**MSB 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.	MSB	Tills vidare	Förordning med instruktion för MSB Enisa Support Action

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

Pelare C 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	Pågående arbete inom ramen för myndighetens ordinarie uppgifter
13:2	**MSB är nationell gemensam kontaktpunkt i enlighet med NIS-direktivet.** Syfte: Genom rollen som nationell gemensam kontaktpunkt bidrar MSB till målet genom att bland annat säkerställa samarbete mellan brottsbekämpande myndigheter och dataskyddsmyndigheter.	MSB	2025	Förordning med instruktion för MSB Lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174) Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster NIS 2-direktivet
13:3	**Polismyndigheten deltar i samarbete med finans- och transaktionsmarknaderna i arbetet för säkrare betalningar.** Syfte: Att förebygga cyberbrott inom transaktionssystemen.	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndighetens ordinarie uppgifter

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

13:4	**Polismyndigheten deltar i brottsförebyggande nätverk gällande cyberbrott.** Syfte: Att genom bred samverkan öka förmågan att förebygga cyberbrott.	Polismyndigheten	Tills vidare	Pågående arbete inom ramen för myndighetens 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 MSB och flera andra statliga myndigheter skapa bl.a. 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, MSB och Stöldskyddsföreningen	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 myndighetens ordinarie uppgifter

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

	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.			
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	Pågående arbete inom ramen för myndighetens ordinarie uppgifter
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	Pågående arbete inom ramen för myndighetens ordinarie uppgifter.

*Ansvarsfördelningen för det nationella cybersäkerhetsarbetet är under översyn vilket kan påverka ansvarig(a) utförare för flera aktiviteter i föreliggande handlingsplan. Exempelvis kan pågående arbete med kommande nationell lagstiftning som implementerar NIS 2-direktivet i Sverige, samt uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (Fö2024/00786) påverka ansvarsfördelningen för aktiviteterna i handlingsplanen. När detta har slutförts kommer handlingsplanen att uppdateras.

Tryck: Elanders Sverige AB, Vällingby 2025