Regeringens skrivelse 2024/25:121

Nationell strategi för cybersäkerhet 2025–2029

Skr. 2024/25:121

Regeringen överlämnar denna skrivelse till riksdagen.

Stockholm den 20 mars 2025

Ebba Busch

Carl-Oskar Bohlin
(Försvarsdepartementet)

Skrivelsens huvudsakliga innehåll

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

Den nationella strategin för cybersäkerhet 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 utgår från tre pelare som anger inriktning för Sveriges cybersäkerhetsarbete:

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

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

Till strategin kopplas bland annat en handlingsplan (bilaga 1) med ett antal aktiviteter som svarar mot regeringens inriktning och kraven i NIS 2-direktivet. Handlingsplanen kommer att uppdateras löpande.

Innehållsförteckning

1 Vision

Regeringens vision är ett motståndskraftigt Sverige med en hög nivå av cybersäkerhet[1], där samhällsviktig verksamhet kan upprätthållas även vid cybersäkerhetsincidenter. För att uppnå denna vision krävs ett förstärkt cybersäkerhetsarbete och ett fördjupat och målinriktat samarbete mellan staten, näringslivet och akademin. Sverige ska dra full nytta av internationella samarbeten på cybersäkerhetsområdet inom EU, Nato och bilateralt med partnerländer för att aktivt stärka såväl vår nationella cybersäkerhet som den hos andra medlemsstater, allierade och partners.

Visionen understryker vikten av att få grundläggande och förstärkt cybersäkerhet på plats, samt vikten av fungerande samarbete mellan nyckelaktörer inom cybersäkerhetsområdet, såväl i fredstid som i krig. Ett välfungerande Nationellt cybersäkerhetscenter (NCSC) som bidrar till att samordna samhällets arbete med att stärka den nationella cybersäkerhetsförmågan behövs och kommer också sektorsansvariga myndigheter till gagn i deras arbete med att ta fram välanpassade krav. Detta är en grundförutsättning för hög cybersäkerhet och höjer den nationella förmågan att förebygga, förbereda sig för, förstå, bemöta och utvärdera cybersäkerhetsincidenter. Det bidrar också till en robust bas för det civila försvaret och till ett effektivt cyberförsvar samt bidrar till att stärka svenska företags position och konkurrenskraft.

Allt detta ska sammantaget leda till ett säkrare Sverige.

2 Den nationella cybersäkerhetsstrategins utgångspunkter

Den nationella strategin för cybersäkerhet utgår från nationella behov och från NIS 2-direktivet[2] och dess allriskperspektiv för att hantera en bredd av utmaningar såsom kompetensbrist, komplex reglering, sårbara leveranskedjor och bristande systematiskt cybersäkerhetsarbete. Mot bakgrund av det säkerhetspolitiska läget fokuserar strategin därtill i vissa delar särskilt på antagonistiska hot i hela hotskalan.[3] Strategin ersätter den tidigare strategin Nationell strategi för samhällets informations- och cybersäkerhet (skr. 2016/17:213).

Ett systematiskt och riskbaserat cybersäkerhetsarbete hos samhällets alla organisationer utgör, tillsammans med säkerhetsskydd och cyberförsvar, Sveriges nationella motståndskraft på cybersäkerhetsområdet. Organisationer används i denna strategi som samlingsbegrepp och avser allt från statliga myndigheter och statligt ägda

[1] *Cybersäkerhet:* denna strategi använder likt NIS 2-direktivet termen ”cybersäkerhet” i stället för termen ”informations- och cybersäkerhet”.

[2] 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).

[3] I avsnitt 3 Cybersäkerhetslandskapet redogör regeringen för ett antal olika utmaningar,

bolag till bland annat kommuner, regioner och privata och kommunala bolag. Med ett systematiskt cybersäkerhetsarbete åsyftas att skyddsåtgärder prioriteras systematiskt och utifrån en bedömning av vilka risker som är mest sannolika och har störst potentiell påverkan. Säkerhetsskydd avser skydd av säkerhetskänslig verksamhet mot spionerі, sabotage, terroristbrott och andra brott som kan hota verksamheten samt skydd i andra fall av säkerhetsskyddsklassificerade uppgifter. Säkerhetsskydd inkluderar även de skyddsåtgärder som genomförs inom informations- och cybersäkerhetsområdet för att upprätthålla säkerhetsskyddet. Säkerhetsskyddslagen (2018:585) och säkerhetsskyddsförordningen (2021:955) gäller bland annat för den som till någon del bedriver verksamhet som är av betydelse för Sveriges säkerhet. 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 i dag som mark-, sjö-, luft- och rymdoperationer. I fredstid kan Försvarsmaktens cyberförsvarsresurser användas för att stödja samhället under kriser eller andra allvarliga händelser.

Fördjupningsruta – Ansvarsprincipen gäller även på cyberområdet
Vid en cybersäkerhetsincident kan en krissituation uppstå som konsekvens och ansvarsprincipen därmed bli tillämplig inom den offentliga förvaltningen. Principen innebär att den som i normala fall ansvarar för en verksamhet, till exempel en statlig myndighet eller kommun, också har detta ansvar under en krissituation.[4]

2.1 Målgrupp

Den nationella strategin för cybersäkerhet och den tillhörande handlingsplanen ska vara av värde för hela samhället och alla typer av organisationer, såväl deras ledningar som de funktioner som arbetar med cybersäkerhet. Strategins primära målgrupp är dock myndigheterna med särskilt ansvar för verksamhet som bedrivs inom ramen för NCSC, och tillsynsmyndigheter inom den samlade cybersäkerhetsregleringen samt andra organisationer som ingår i beredskaps- och NIS 2-sektorerna.

2.2 Nationell politik för cybersäkerhet

Cybersäkerhet är ett område som sträcker sig över flera fält, politikområden och sektorer. Cybersäkerhetsfrågorna kräver således ett tvärsektoriellt arbete utifrån en rad olika kompetenser. Denna strategi kommer att utgöra regeringens långsiktiga inriktning för det systematiska arbetet med cybersäkerhet tillika regeringens politik för cybersäkerhet. Regeringens arbete med att stärka och bidra till Sveriges cybersäkerhet

[4] I särskilda fall, till exempel vid det som i NIS 2-direktivet benämns storskaliga cybersäkerhetsincidenter och kriser, ska dock en eller flera behöriga cyberkrishanteringsmyndigheter ansvara för nationell hantering. Detta gäller till exempel omfattande eller gränsöverskridande incidenter.

återspeglar sig även i bland annat propositionen Totalförsvaret 2025–2030 (prop. 2024/25:34). I propositionen konstateras det att informations- och cybersäkerhet är en viktig förutsättning för hela totalförsvaret inklusive det militära cyberförsvaret. Vidare betonas vikten av att Försvarsmakten i fred kan bidra till cybersäkerhetsarbetet. Utrikes- och säkerhetspolitiska aspekter av cyberfrågor behandlas primärt i regeringens strategi Sverige i en digital värld – en strategi för Sveriges utrikes- och säkerhetspolitik inom cyberfrågor och digitala frågor (UD2024/16802). Den strategin och den nationella strategin för cybersäkerhet är ömsesidigt förstärkande. De båda strategierna har flera beröringspunkter. Exempelvis utgör nationell förmåga inom lägesmedvetenhet, attribuering och svarsåtgärder en viktig del i utrikes- och säkerhetspolitiskt bemötande av cyberhotaktörer. Koordinering av utrikes- och säkerhetspolitiken med åtgärder på nationell nivå är en förutsättning för samlad hantering av så kallade offentliga utpekanden och bidrar till stärkt medvetenhet och motståndskraft.

Regeringens nationella säkerhetsstrategi (skr. 2023/24:163) sätter ramarna för arbetet med nationell säkerhet. Den beskriver de prioriteringar och principer som ligger till grund för Sveriges säkerhet och är utgångspunkten för de överväganden som görs i denna strategi. Den nationella säkerhetsstrategin anger att åtgärder för att samhällsviktiga och samhällskritiska verksamheter ska bli mer motståndskraftiga mot allvarliga störningar i fredstid är en prioriterad del av arbetet med att stärka det civila försvaret. Samtidigt betonar regeringen i den nationella säkerhetsstrategin att Sveriges nationella säkerhet är en angelägenhet för alla i vårt samhälle. En målbild är även att säkerhetshotet från auktoritära stater som Kina, Ryssland och Iran prioriteras och hanteras i samarbete med demokratiska länder. Av strategin framgår att regeringen avser att stärka förmågan att identifiera, hantera och bemöta hybridhot och angrepp, inklusive cyberangrepp.

Regeringen inledde under 2023 ett arbete med att utveckla NCSC med målet att centret bland annat ska utgöra navet i det nationella cybersäkerhetsarbetet. Under 2023 tillsattes en så kallad bokstavsutredning med uppdrag att se över centrets verksamhet (Fö 2023:A). Utifrån den utredningen har regeringen beslutat att NCSC från och med 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 och berörs därför inte närmare i denna strategi.

I NIS 2-direktivet fastställs åtgärder för att uppnå en hög gemensam cybersäkerhetsnivå i hela unionen. Regeringen tillsatte under 2023 en utredning för att bland annat föreslå de anpassningar av svensk rätt som bör göras till följd av direktivet och utredningen överlämnade i mars 2024 sitt delbetänkande (SOU 2024:18). Ansvarsförhållanden för de aktörer som omfattas av NIS 2-direktivet kommer att definieras i nationell reglering som införlivar direktivet i Sverige. I strategins bilaga 2 ges en nulägesbeskrivning av de centrala aktörer som har särskilda roller och ansvar att bedriva tillsyn, stötta och samordna arbetet med cybersäkerhet.[5]

[5] Bilagan utgår till del från den nationella reglering som införlivade NIS-direktivet och kommer att uppdateras när bland annat implementeringen av NIS 2-direktivet har fastställt ansvarsförhållandena inom svensk cybersäkerhet.

Utöver denna cybersäkerhetsstrategi avser regeringen även att ta fram en strategi i enlighet med CER-direktivet[6,7]. Cybersäkerhetsområdet har dessutom naturliga kopplingar till frågor om digital omställning och digital infrastruktur, vilket kommer att beröras ytterligare i regeringens kommande digitaliseringsstrategi.

2.3 Internationell kontext för nationell cybersäkerhet

Sveriges cybersäkerhet och reglering på området styrs delvis nationellt men också i ökande grad av den internationella kontexten. Sveriges cybersäkerhetspolitik påverkas av internationell reglering, styrande dokument, policyer och standarder. 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 NIS 2-direktivet. Vidare finns cyberresiliensförordningen[8] och cybersäkerhetsakten[9], 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. Den civil-militära kopplingen inom cybersäkerhetsfrågor understryker vikten av ett samordnat utvecklingsarbete mellan Nato och EU inom cybersäkerhet och cyberförsvar.

Det finns vidare internationella konventioner och avtal som i varierande grad ställer krav på och reglerar frågor om cybersäkerhet för Sverige. Omvänt gäller också att Sverige ställer krav på partnerländer. Att folkrätten gäller i cyberrymden har fastslagits i flera rapporter som antagits av FN:s generalförsamling[10]. Inom FN har det dessutom utarbetats icke-bindande normer för ansvarsfullt statligt uppträdande i cyberrymden. Frågor om hur folkrätten ska tillämpas i olika avseenden diskuteras fortsatt bland annat i FN-sammanhang. Sverige publicerade i juli 2022 en nationell position om folkrätten i cyberrymden och EU:s medlemsstater enades i november 2024 om en deklaration om samma fråga.

[6] Europaparlamentets och rådets direktiv (EU) 2022/2557 om kritiska entiteters motståndskraft och om upphävande av rådets direktiv 2008/114/EG (CER-direktivet).
[7] CER- och NIS 2-direktiven kompletterar varandra och ställer krav på samstämmighet. Exempelvis ska entiteter som identifierats som kritiska enligt CER-direktivet anses vara väsentliga enligt NIS 2-direktivet. Vidare ska nationella strategier antas som innehåller bland annat strategiska mål i syfte att uppnå och upprätthålla en hög cybersäkerhetsnivå (NIS 2) respektive en hög grad av motståndskraft (CER).
[8] Europaparlamentets och rådets förordning (EU) 2024/ 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).
[9] 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).
[10] Se till exempel resolution A/RES/76/19.

3 Cybersäkerhetslandskapet

Sveriges cybersäkerhet påverkas av ett antal sårbarheter som kan ha olika ursprung och manifestera sig inom ett antal områden. Dessa sårbarheter kan samlat eller var för sig utgöra strategiska sårbarheter i ett digitaliserat samhälles cybersäkerhetslandskap och riskera att påverka samhällsviktig verksamhet och ytterst Sveriges säkerhet. Sårbarheter är vanligt förekommande och kan bland annat röra organisatoriska, tekniska, infrastrukturella och mänskliga faktorer.

Sverige står också, likt andra länder, inför en dynamisk och föränderlig hotbild där cyberhotaktörer kontinuerligt utvecklar nya metoder och anammar ny teknik. Såväl att upptäcka sofistikerade cyberangrepp som att definitivt attribuera angrepp till en specifik hotaktör är komplext och bidrar till att cyberangrepp ofta innebär låg risk för påföljder, motåtgärder eller personliga konsekvenser för hotaktörer.

I det följande redogörs dels för ett antal typiska hotaktörer, dels för sårbarheter, som påverkar Sveriges cybersäkerhet. Såväl sårbarheter som antagonistiska hot kan leda till allvarliga konsekvenser. När en incident inträffar kan det också vara svårt att direkt avgöra om skälet är yttre påverkan eller annat fel. Det ska även framhållas att gränsen mellan statliga, kriminella och andra grupperingar ofta är svår att dra. Det finns flera exempel på aktörer inom organiserad brottslighet med nära, men dolda, kopplingar till antagonistiska statliga aktörer.

3.1 Hot från statliga aktörer

Cyberangrepp utförda av statliga[1] eller statsunderstödda[2] aktörer mot svenska verksamheter har ökat i omfattning och kan få allvarliga konsekvenser. Statliga aktörer har sofistikerade offensiva cyberförmågor som bland annat kan användas för teknikstöld, underrättelseinhämtning eller annan verksamhet som tillfälligt stör eller förstör hela eller delar av system, ofta inom kritisk infrastruktur och samhällsviktig verksamhet. Cyberangrepp kan frikopplat från, eller inför eller under, en väpnad konflikt komplettera politiska, diplomatiska, ekonomiska, militära och andra medel som en hotaktör nyttjar. Statliga aktörer bedriver också informationspåverkan, bland annat med stöd av cyberangrepp, och nyttjar det fria informationsflödet på internet för antagonistiska syften. Den breda palett av metoder som aktörer använder för att påverka Sverige kan samlas under rubriken hybridhot. Genom sådana hot eftersträvar en motståndare att utnyttja alla sårbarheter i vårt samhälle för att bland annat uppnå sina politiska mål. Cyberangrepp i olika former är en ofta förekommande metod i dessa hybridaktiviteter. God cybersäkerhet försvårar således för hotaktörer att utöva hybridsaktiviteter mot Sverige och svenska intressen.

[1] Statliga aktörer drivs direkt av underrättelse- och säkerhetstjänster eller deras täckföretag alternativt genom organisationer och icke-organiserade individer som agerar ombud.
[2] Statliga aktörer kan också understödja kriminella grupperingar baserade i det egna landet eller härrörande från länder som gör lite eller inget alls för att förhindra sådan kriminell verksamhet.

3.2 Hot från cyberaktivister

Cyberaktivister använder cyberangrepp som metod för att främja politiska eller ideologiska syften bland annat genom att exponera eller manipulera data. Cyberaktivister kan, baserat på politiska eller ideologiska motiv, sympatisera med eller agera för olika statsaktörer.

3.3 Hot från cyberbrottslighet och kriminella grupperingar

Antalet kriminella grupperingar som ägnar sig åt cyberbrottslighet[3] i form av angrepp på it-system har stadigt ökat. En allt större andel brott begås i digitala miljöer eller med hjälp av digitala verktyg. It-beroende brottslighet kan utgöra hot mot såväl individer, företag och andra organisationer som samhället i stort, där ransomware-angrepp och datastölder är särskilt utmärkande. Denna typ av brottslighet kan få stora konsekvenser för enskilda och leder till stora kostnader för såväl privata som offentliga aktörer. Överbelastningsangrepp utförda av kriminella grupperingar riskerar också att påverka viktiga digitala samhällsfunktioner och förtroendet för dessa funktioner. Både kriminella aktiviteter som initieras av de kriminella grupperingarna själva på eget initiativ och sådana som utförs på uppdrag av någon annan mot betalning,[4] spelar en betydande roll i det it-kriminella ekosystemet.

Cyberbrottslighet är gränsöverskridande och drar nytta av nya verktyg, exempelvis baserade på generativ AI och nya kommunikationstjänster. Information som krävs inom ramen för brottsutredningar finns ofta i andra länder, vilket försvårar brottsbekämpande myndigheters möjligheter till lagföring.

3.4 Brister i cybersäkerhetsarbetet

Många organisationer har brister i sitt förebyggande systematiska cybersäkerhetsarbete vilket medför att grundläggande säkerhetsåtgärder inte implementeras. Detta utgör en strategisk sårbarhet. Bland annat små kommuner och mindre aktörer, såsom små och medelstora företag, kan sakna ett tillfredsställande cybersäkerhetsarbete av bland annat resurs- och kompetensskäl. Kunskapsnivån om vad som är skyddsvärt i den egna verksamheten är dessutom ofta låg och många verksamhetsutövare har utmaningar i arbetet med att identifiera vilka delar av verksamheten som är säkerhetskänslig, samhällskritisk eller både och, inte minst ur ett tillgänglighetsperspektiv. Detta gör det svårt att ta medvetna beslut om informationshantering i allmänhet och dimensionering av skyddsåtgärder i synnerhet.

[3] Cyberbrottslighet kan delas upp i två olika typer: it-beroende (cyber dependent) och it-relaterad (cyber enabled). It-beroende brott är till exempel ransomware och DDoS, medan it-relaterade är traditionella brott som använder sig av it, till exempel bedrägerier och illegal försäljning på nätet.

[4] Benämns i vissa sammanhang Crime as a service, CaaS.

Organisationer som saknar tillräckligt förebyggande cybersäkerhetsarbete brister ofta även i analyser över vilka krav deras it-system behöver uppfylla baserat på verksamhetens behov. För att effektivt följa lagkrav och uppnå den förbättring som lagstiftaren avsett, krävs att organisationer genomför en grundlig verksamhetsanalys som komplement. Denna analys kan i sig vara komplex och omfattande, särskilt för organisationer som ansvarar för vitt skilda verksamheter och därmed har olika regleringar och krav att förhålla sig till.

3.5 Komplex reglering

Ökad reglering på cybersäkerhetsområdet ställer nya krav på organisationer att hantera cyberrelaterade verksamhetsrisker. Ett systematiskt arbete med cybersäkerhetsrisker stärker vanligen organisationers verksamhet och kan på lång sikt även vara kostnadsbesparande. Samtidigt kan betungande reglering också leda till kostnader för såväl privatpersoner och offentliga aktörer som enskilda näringsidkare. Olika regleringar, såväl nationella som internationella, kan samlat innehålla överlappande krav som är svåra att sortera bland, och som skapar utmaningar i att göra adekvata prioriteringar. Detta är särskilt fallet för mindre aktörer som små och medelstora företag med begränsade resurser. Det statliga cybersäkerhetsarbetet är dessutom uppdelat i olika, delvis överlappande ansvarsområden vilket medför att olika statliga myndigheter ansvarar för tillsyn, föreskrifter och vägledning enligt olika regelverk. Detta riskerar att försvåra för enskilda företag och organisationer att följa reglerna.

3.6 Kompetens- och kunskapsbrist

Kompetensförsörjning inom cybersäkerhetsområdet har under en lång tid varit en utmaning. Utöver brister i allmän cybersäkerhetskompetens råder det brist på både cybersäkerhetsexperter och personal med relevant utbildning och arbetslivserfarenhet inom angränsande områden såsom säkerhetsskydd och säkerhet inom så kallad operativ teknik[5], även kallat OT-säkerhet. Denna brist, som även är global, påverkar såväl offentlig som privat sektor. Därtill är den generella kunskapen om cybersäkerhet ofta begränsad hos yrkesroller såsom chefer, jurister, upphandlare och it-utvecklare vilka också sällan arbetar direkt med frågorna. Teknikutveckling och digital omställning bidrar till ett ständigt ökande behov av forskning, kompetens och färdigheter på området. Brist på generell cybersäkerhetskompetens hos organisationer kan dessutom leda till att tydliga krav inte ställs på de för verksamheten viktiga it-systemen. Vidare medför ökad och utvecklad reglering inom cybersäkerhet och säkerhetsskydd samt den återupptagna totalförsvarsplaneringen nya kompetensbehov för både tillsynsmyndigheter och verksamhetsutövare.

[5] Sådana system kan också benämnas cyberfysiska system eller industriella styr- och informationssystem.

Svensk cybersäkerhetsforskning är konkurrenskraftig och det bedrivs framstående forskning vid flera universitet och högskolor. Samtidigt som ett fåtal forskningsområden inom cybersäkerhet är dominerande bedrivs forskning inom andra angelägna cybersäkerhetsfrågor enbart i begränsad omfattning och tvärvetenskapliga perspektiv saknas ofta. Vidare har koordinering inom cybersäkerhetsforskningen i Sverige ofta saknats.

3.7 Bristande incidenthantering

Adekvata arbetssätt för incident- och kontinuitetshantering saknas hos många organisationer och få övar dessa förmågor. Bristande incidenthantering utgör en allvarlig risk för organisationer, särskilt i en tid av ökade cyberhot. Svaga processer ökar organisationers sårbarhet vid cybersäkerhetsincidenter. Bristfällig incidenthantering kan öka risken för förlust av känslig information, förlust av förmågan att tillhandahålla kritiska tjänster och finansiella förluster samt skada förtroendet för en verksamhet.

Cybersäkerhetsincidenter som omfattas av incidentrapporteringskrav ska också rapporteras till behöriga statliga myndigheter, men ett mörkertal i rapporteringen har länge varit en realitet nationellt och internationellt. Detta påverkar möjligheten att skapa en operativ lägesbild och varna andra organisationer, vilket riskerar att förvärra en uppstådd kris. Det minskar också möjligheterna att dra lärdomar och inrikta det förebyggande arbetet.

Mörkertalet i antalet rapporterade cyberbrott försvårar också brottsbekämpande myndigheters förebyggande arbete, operativa hantering och utredning vid cybersäkerhetsincidenter. I förlängningen påverkas möjligheten att lagföra den som har utfört en brottslig handling. Det finns inte någon skyldighet att polisanmäla cyberbrott. Detta ställer krav på skyndsam informationsdelning mellan de myndigheter som tar emot incidentrapportering och brottsbekämpande myndigheter för att öka möjligheten att följa upp brott och att säkra bevis.

3.8 Outvecklad informationsdelning mellan den privata och offentliga sektorn

Organisationer är beroende av varandra för att förebygga, uppmärksamma och hantera sårbarheter, hot och cybersäkerhetsincidenter. Privata och offentliga organisationer har tillgång till olika informationsflöden. Expert- och tillsynsmyndigheter tar exempelvis emot incident- och sårbarhetsrapporter, medan privata organisationer innehar majoriteten av samhällets cyberresurser och är centrala för nationell cybersäkerhetsförmåga. Informationsdelning och samarbete mellan och inom privat och offentlig sektor kräver bland annat uppbyggda kommunikationsvägar och adekvata processer samt tillit aktörer emellan. Dessa processer behöver bland annat utgå ifrån och ta hänsyn till privata aktörers affärsintressen och sekretess för affärs- och driftförhållanden. Outvecklat och bristande samarbete mellan det privata och offentliga, nationellt såväl som internationellt, utgör en sårbarhet.

3.9 Sårbara leveranskedjor, beroenden och produkter

Incidenter i digitala leveranskedjor, såsom vid systemfel hos leverantörer, kan leda till konsekvenser utanför den organisation som initialt drabbats och kan orsaka störningar i samhällskritiska funktioner. Dagens komplexa beroenden medför dessutom svårigheter att kartlägga sårbarheter i digitala leveranskedjor och försvårar ansvarsutkrävande.

Svag cybersäkerhet hos leverantörer riskerar att påverka säkerheten hos kundorganisationer. Givet att många organisationer är beroende av externt levererade it-driftstjänster, blir organisationer som inte beaktat denna omständighet i sina riskanalyser sårbara om en leverantör misslyckas med att leverera sin tjänst. I sådana fall riskerar organisationen att sakna alternativa lösningar. Det kan vidare innebära allvarliga risker om många organisationer är beroende av samma tjänst eller system.[6] Vid sådan oligopol- eller monopolställning minskas också kundens flexibilitet och valmöjligheter, till exempel möjligheten att nyttja alternativa tjänster vid pågående incidenter. Beroenden av digitala produkt- och tjänsteleveranser från organisationer baserade i tredjeland, kan både vara olämpliga och utgöra en sårbarhet som kan användas som politiskt påtryckningsmedel.

Osäkra digitala produkter med låg cybersäkerhet utgör en stor risk för både nationella och internationella leveranskedjor. Osäkerhet och risker uppstår även ofta vid uppdateringar av hård- och mjukvara. På EU-nivå har detta identifierats som nödvändigt att åtgärda och är i fokus för cyberresiliensförordningen som syftar till att höja tillverkares och leverantörers ansvar för cybersäkerhet och att produkter med digitala element placeras på inre marknaden med färre sårbarheter.[7] Utveckling och bred användning av internationella säkerhetsstandarder på teknik- och cybersäkerhetsområdet kan också bidra till mer robusta leveranskedjor. Utvecklingen av internationella standarder präglas dock i ökad grad av geopolitisk konkurrens.

3.10 Utmaningar kopplat till utvecklingen i digital infrastruktur och digitala tjänster

Sveriges digitala infrastruktur utvecklas kontinuerligt. Nya generationers mobilnät rullas ut och rymden är också en infrastrukturdomän för mobildatakommunikation. Behoven av tillförlitlig och säker digital infrastruktur samt digitala tjänster växer i betydelse och omfattning. Det skapar många nya möjligheter, men ställer också höga krav på både

[6] Okända brister hos och/eller brister i kravställning mot en it-leverantör som levererar it-stöd till många organisationer riskerar att leda till stora störningar inom såväl privat som offentlig sektor i Sverige. Konsekvensen av att licensavgifter höjs, eller att tjänster upphör, riskerar också bli stora.

[7] Den inre marknadens sårbarhet för låg cybersäkerhet är också i fokus för certifieringsramverket som etablerats i cybersäkerhetsakten. Möjligheten att genom certifiering visa uppfyllnad av cybersäkerhetskrav finns reglerat i flera EU-akter såsom NIS 2-direktivet, cyberresiliensförordningen, AI-förordningen och den reviderade eIDAS-förordningen.

upphandlingsförmåga och en väl utvecklad hantering av sårbarheter och beroenden för såväl privata som offentliga alternativ.

3.11 Utmaningar med uppkoppling av enheter och infrastruktur

Processer inom kritisk infrastruktur[8] som tidigare varit manuella eller mekaniska har med tiden digitaliserats alltmer. Denna utveckling förstärks av framväxten av nya så kallade IoT-enheter, som ständigt är uppkopplade, och som kan användas bland annat för att styra och övervaka processer. De system som används inom kritisk infrastruktur har tekniska förutsättningar som särskiljer dem från traditionella it-system och gör dem komplexa att skydda. Säkerhetsarbete inom OT-säkerhet utgör därför en utmaning, bland annat mot bakgrund av kompetensbristerna på området.

IoT-enheter med svag säkerhet kan medföra betydande cybersäkerhetsrisker och kan om de är anslutna till organisationers övriga it-infrastruktur utlösa cybersäkerhetsincidenter. Även för privatpersoner kan IoT-konsumentprodukter med låg säkerhet innebära risker. Sådana produkter kan också nyttjas i botnätverk och användas av hotaktörer för överbelastningsattacker mot andra organisationer.

3.12 Teknikutvecklingen

Utveckling av strategiskt viktig teknik skapar möjligheter för Sverige. Teknikutveckling kan påverka samhällets säkerhet. Till exempel kan användning av AI-funktioner effektivisera cybersäkerhetsarbetet. Samtidigt kan AI användas för att genomföra cyberangrepp och desinformationskampanjer med bredare spridning. Cybersäkerhetsincidenter i AI-system får också ökade konsekvenser i takt med att samhällets beroende av sådana system ökar.

Utveckling av kvantteknik och kraftfulla kvantdatorer gör vissa kryptografiska algoritmer alltmer sårbara för forcering. Genom bland annat cyberangrepp, avlyssning och annan underrättelseinhämtning kan kvalificerade hotaktörer få tillgång till krypterade data som de lagrar i syfte att kunna forcera när kvanttekniken i framtiden utvecklats.

[8] Kritisk infrastruktur innefattar bland annat tjänster och tillhandahållare av dessa inom sektorerna finans, transport, energi och elektronisk kommunikation. Det kan också handla om it-infrastruktur som används brett inom statlig och kommunal förvaltning. Denna uppräkning ska dock inte ses som uttömmande eller som en legal definition. Kritisk infrastruktur innefattar en mängd verksamheter, varav många omfattas av NIS 2-direktivet, säkerhetsskyddsregleringen eller andra sektorsspecifika unionsrättsakter som innehåller motsvarande cybersäkerhetskrav såsom Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011.

4 Regeringens inriktning

Strategin utgår från tre pelare som anger inriktning för Sveriges cybersäkerhetsarbete:

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

Pelarna innehåller i sin tur ett antal mål med tillhörande resultatindikatorer. Strategins mål tar sikte på ett antal områden för att åstadkomma förflyttningar och bemöta de hot och sårbarheter som återfinns i avsnitt 4. Målen i strategin sträcker sig till och med 2029. För respektive mål finns en inledning som beskriver målet och sätter det i sitt sammanhang. Därefter presenteras under rubriken ‘Önskat läge 2030’ 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 uppföljning av dessa.

Till strategins pelare och mål kopplas en handlingsplan (bilaga 1) med ett antal 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.

4.1 Pelare A: Systematiskt och effektivt cybersäkerhetsarbete

Pelaren *Systematiskt och effektivt cybersäkerhetsarbete* handlar om att öka svensk motståndskraft genom att ge förutsättningar för alla samhällets organisationer att stärka sitt systematiska cybersäkerhetsarbete, om att öka säkerheten i digitala leveranskedjor och produkter, och om att skydda kritiska system och verksamheter.

Utöver aktiviteterna i handlingsplanen gäller följande övergripande resultatindikatorer för pelare A:

- 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.

4.1.1 Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer

Ett robust samhälle har behov av väl fungerande it-system varför grundläggande cybersäkerhetsarbete skapar förutsättningar för att hantera fredstida kriser och ytterst krig. I ett digitaliserat samhälle behöver därför alla organisationer ha ett fullgott, systematiskt säkerhetsarbete och som en del av detta implementera cybersäkerhetsåtgärder. Respektive organisations ledning har det yttersta ansvaret för sin verksamhet och därmed dess cybersäkerhet. Kraven i NIS 2-direktivet på att ledningsorgan ska godkänna riskhanteringsåtgärder för cybersäkerhet och övervaka deras genomförande samt genomgå utbildning lägger en god grund, men måste i sin tur baseras på en grundläggande förståelse för hur verksamheten kan påverkas av en cyberrelaterad incident.

Önskat läge 2030:
Organisationer som bedriver samhällsviktig verksamhet genomför noggranna verksamhetsanalyser för att identifiera vilken cybersäkerhetsförmåga som är nödvändig för att garantera organisationens verksamhet. Berörda statliga myndigheter har genom aktivt deltagande i EU-samarbetet kring NIS 2-direktivets krav tagit fram nationellt anpassade vägledningar och stöd. Tillsammans med relevanta standarder stöttar berörda statliga myndigheters vägledning organisationers anpassning till NIS 2-direktivets krav och därigenom införandet av proportionella säkerhetsåtgärder. NIS 2-direktivets kravnivå får genomslag även hos organisationer som inte omfattas av direktivet, särskilt organisationer med samhällskritisk funktion som redan omfattas av reglering med omfattande krav men som saknar allriskperspektiv. Sektorsspecifika cybersäkerhetsakter, som till exempel DORA-förordningen[1], tillämpas och utvidgar kraven på motståndskraft till ytterligare aktörer. En grundläggande cyberhygien är en integrerad del i all samhällsviktig verksamhet och en ökad cybersäkerhetsmognad inom alla samhällskritiska sektorer är uppnådd. Offentliga aktörer och företag, oavsett storlek, arbetar aktivt med kontinuitetsplanering som en central del av sin beredskap.

Alla organisationer har förutsättningar för och tar ansvar för att skydda sin information och de nätverks- och informationssystem som används för verksamheten eller för att tillhandahålla tjänster. Även tillgång till information samt till funktioner och förmågor upprätthålls. Skyddet dimensioneras utifrån såväl verksamhetens och informationens säkerhetsbehov som reglerade krav och stöttas av välutvecklat stöd och vägledning från de statliga myndigheter som har i uppgift att ge sådant stöd. Organisationer har en planering för vilken verksamhet som alltid behöver kunna upprätthållas vid störningar eller incidenter. Privat-offentlig samverkan har utvecklats inom flera sektorer för att spegla privata aktörers alltmer centrala ställning för nationell säkerhet. Berörda statliga myndigheter erbjuder utbildning till ledningsorgan inom samhällsviktig verksamhet och beredskapsorganisationer.

[1] Europaparlamentets och rådets förordning (EU) 2022/2554 om digital operativ motståndskraft för finanssektorn (DORA).

En gemensam och dimensionerad nationell cybersäkerhet som bygger på reglerad kravställning, fastställda säkerhetsnivåer och nationellt kravställda produkter och tekniska lösningar har implementerats i skyddsvärda verksamheter såväl offentligt som privat.

4.1.2 Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering

Att den offentliga sektorn kan säkerställa en hög nivå av cybersäkerhet är avgörande för att upprätthålla ett högt förtroende för offentliga institutioner. Statliga myndigheters, kommuners och regioners förutsättningar och resurser att bedriva ett fullgott cybersäkerhetsarbete skiljer sig samtidigt åt. Rysslands fullskaliga invasion av Ukraina har också aktualiserat frågan om statens förmåga att upprätthålla samhällsviktiga tjänster och kritisk infrastruktur samt skydda viktiga grunddata även i kris och ytterst krig.

Önskat läge 2030:
Berörda statliga myndigheters verktyg för cybersäkerhetsmätningar utvecklas och får större genomslag i att stödja andra organisationer med att kartlägga det interna cybersäkerhetsarbetet. Tillhörande råd om vilka åtgärder som organisationer, utifrån deras resultat i cybersäkerhetsmätningar, bör vidta har utvecklats och fått större genomslag. Kraven i den svenska reglering som genomfört NIS 2-direktivet har lagt en god grund för att höja cybersäkerheten i den offentliga förvaltningen vilket också framgår i förmågebedömningar av aktörernas cybersäkerhet inom det civila försvaret. Enhetliga säkerhetskrav och säkerhetsnivåer i den offentliga sektorn främjar upprätthållandet av cybersäkerhet i hela hanteringskedjan och en gemensam stark cybersäkerhet.

Statliga myndigheter erbjuder samordnade, säkra och i möjligaste mån kostnadseffektiva alternativ för gemensam digital infrastruktur och it-tjänster, vilket har underlättat för aktörer med bristande cybersäkerhetsförmåga och bidragit till att säkerställa samhällsfunktioner genom hela konfliktskalan. Ramavtal finns på plats med cybersäkerhetskrav som skyddar konfidentialitet, riktighet och tillgänglighet. Upphandling med adekvata krav resulterar i avtal med robusta säkerhetskrav som leder till väl fungerande tjänster, säker hantering av information, samt innovation inom säkerhetsområdet. Sammantaget tryggas samhällets tilltro till att rätt information alltid finns tillgänglig för rätt part.

Statliga myndigheters nationella insatser kring tekniskt stöd är kostnadseffektiva och möter målgruppens behov. Fler kollektiva tekniska säkerhetslösningar erbjuds centralt och stöttar särskilt cybersäkerheten hos små organisationer i myndighetssektorerna och i kommuner och regioner där information som är av betydelse för samhällskritisk och samhällsviktig verksamhet återfinns. Kommuner och regioner har identifierat och implementerat fler effektiva gemensamma metoder för att höja sin kollektiva cybersäkerhet.

4.1.3 Mål 3: Stärkt cybersäkerhetsarbete inom kritisk infrastruktur

Att kritisk infrastruktur kan upprätthållas är nödvändigt för samhällets säkerhet och stabilitet. Många av de tjänster och funktioner som utgör kritisk infrastruktur tillhandahålls av privata organisationer. Cybersäkerhetsarbetet för operatörer av kritisk infrastruktur behöver bland annat därför utgå från verksamheternas individuella förutsättningar, men också från deras särskilda sårbarheter och den specifika hotbild som riktas mot den aktuella verksamheten. Samhällets beroende av dessa verksamheter gör deras cybersäkerhetsarbete centralt. Stärkt cybersäkerhetsarbete bidrar också till att försvåra för hotaktörer att rikta cyberattacker mot kritisk infrastruktur som en del av hybridaktiviteter för att påverka Sverige.

Önskat läge 2030:
Operatörers skydd av kritisk infrastruktur, inklusive säkerhetsarbetet inom OT, dimensioneras utifrån infrastrukturens samhällsbetydelse och antagonistiska hotbild. Säkerhetsövervakning av it- och OT-system inom kritisk infrastruktur stimuleras. Sektorsansvariga myndigheter enligt NIS 2-regelverket samt andra berörda statliga myndigheter nyttjar NCSC:s råd och stöd inom cybersäkerhet för att sektorsanpassa vägledningar och andra styrdokument för respektive sektor. Operatörers arbete med att implementera säkerhetsåtgärder stärks därigenom vilket, tillsammans med deras hantering av sårbarheter, leder till höjd motståndskraft. Statliga myndigheter utvecklar stöd för skydd av kritisk infrastruktur. NIS 2- och beredskapsorganisationer tillgodogör sig det stöd och den utbildning som erbjuds inom säkerhet för kritisk infrastruktur. Samarbetet och informationsdelningen mellan statliga myndigheter och operatörer av kritiska system har utvecklats och sammanlänkar sektorer, utifrån att sektorer ofta har tydliga överlapp och beroenden sinsemellan. Övnings- och testverksamhet som möjliggörs genom bland annat cyber range-miljöer fortsätter utvecklas och nyttjas i bred utsträckning. Sektorsspecifika samarbetsforum har fortsatt en central roll när det gäller samverkan, övningsverksamhet och informationsdelning, och ett ökat samarbete sker mellan statliga myndigheter och näringslivet.

4.1.4 Mål 4: Robustare digitala leveranskedjor och minskat beroende

Hantering av digitala leveranskedjor, molntjänster och beroenden utgör en central prioritering för regeringens cybersäkerhetsarbete. För att stärka Sveriges cybersäkerhet behöver monoberoenden och kritiska tredjelandsberoenden identifieras och hanteras och digitala leveranskedjor bli mer robusta.

Önskat läge 2030:
Sverige har en hög ambition i det nationella och det internationella arbetet för säkerhet i digitala leveranskedjor, särskilt på EU-nivå. Statliga myndigheter ger organisationer, såväl privata som offentliga, vägledning

när det gäller inventering av leveranskedjor och utkontraktering. Organisationer inventerar och bedömer säkerheten i sina leveranskedjor samt ställer adekvata cybersäkerhetskrav i avtal med leverantörer. Även de organisationer som inte omfattas av NIS 2-direktivet bedömer beroenden och risker i sina leveranskedjor samt säkerställer nödvändiga reservrutiner.

Bestämmelserna i cyberresiliensförordningen om cybersäkerhet i produkter med digitala element leder till ökad säkerhet i leveranskedjor. Svenska företag som tillämpar säker utveckling av mjukvara och fast programvara samt inbyggd säkerhet är mer konkurrenskraftiga och bidrar till att förse marknaden med produkter med färre säkerhetsbrister. Efterfrågan på säkra produkter bland organisationer i Sverige har ökat, pådrivet av högre och bättre kravställning från den offentliga sektorn när det gäller tjänster och produkters funktion. Sverige slår vakt om fortsatt inflytande inom internationell standardisering och bidrar till välanpassade internationella standarder som främjar säkra leveranskedjor. Berörda statliga myndigheter, i samarbete med näringslivet, verkar bland annat för att nya standarder och europeiska certifieringsordningar för cybersäkerhet utvecklas transparent samt att svenska behov och prioriteringar får genomslag. Organisationer nyttjar cybersäkerhetscertifierade it-tjänster och produkter utifrån sin riskbedömning.

4.1.5 Mål 5: Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete

Regleringen på området kommer kontinuerligt att öka och i takt med växande systemintegration, där fler aktörer blir beroende av varandra, är ytterligare reglering och skärpta cybersäkerhetskrav för fler aktörer att vänta. För att höja samhällets cybersäkerhet, är det därför viktigt att så långt som möjligt förenkla organisationers tillämpning av komplexa regler samt att stärka och samordna tillsynsmyndigheters verksamhet. Förenklad regelefterlevnad kan också stärka konkurrenskraften hos företag.

Önskat läge 2030:
Sverige är, med stöd i genomförda nationella åtgärder, en ledande medlemsstat i utvecklingen av nya internationella regelverk inom cybersäkerhet som innehåller proportionerliga och harmoniserade regler. Statliga myndigheters aktiva deltagande i erfarenhetsutbytet på EU-nivå bidrar till harmoniserade NIS 2-krav mellan medlemsstater. NIS 2-direktivets krav har omsatts i ensade regelverk sektorerna emellan och skapat förutsättningar för effektiv regelefterlevnad. Statliga myndigheter är väl koordinerande när det gäller befintlig reglering i syfte att föreskrifter, allmänna råd och vägledningar så långt som möjligt ensas och följer en likartad logik, struktur och terminologi. NCSC:s råd och stöd i cybersäkerhetsfrågor kompletterar sektorsmyndigheternas föreskriftsarbete. Genom kontinuerligt utvecklad tillsynsverksamhet stärks efterlevnaden av cybersäkerhetsregleringen. Myndigheter med centrala roller har rätt befogenheter och mandat.

4.1.6 Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete

Näringslivet står för stora ekonomiska värden kopplat till såväl innovation som produktion och samhällsviktiga tjänster. Små och medelstora företag utgör majoriteten av företagen i Sverige och står sammantaget för en ansenlig del av dessa värden, samtidigt som de generellt sett är mer sårbara än större företag för cybersäkerhetsrisker. När dessa drabbas av cybersäkerhetsincidenter kan omfattande produktionsbortfall, störningar i samhällsviktiga tjänster och ekonomiska konsekvenser uppstå. Vissa små och medelstora företag har god cybersäkerhet, och det finns även ett starkt segment av sådana bolag verksamma inom cybersäkerhetsfältet, men faktorer som bristande cybersäkerhetsmedvetenhet och knappa resurser gör majoriteten av dem sårbara. Dessa löper dessutom ofta stor risk att inte återhämta sig från allvarliga cybersäkerhetsincidenter. Små och medelstora företags motståndskraft och skydd av affärshemligheter är därför en väsentlig del i att slå vakt om Sveriges samlade konkurrens- och motståndskraft.

Önskat läge 2030:
Statliga myndigheter erbjuder i större utsträckning stöd och vägledning som stöttar små och medelstora företag, även till dem som inte omfattas av den svenska reglering som genomfört NIS 2-direktivet. Statliga myndigheters samarbeten med intresse- och företagsorganisationer stimuleras och nyttjas för att motverka digitala brott och öka cybersäkerheten. Teknikföretag tar ansvar för att erbjuda säkra tjänster, vilket indirekt stärker små och medelstora företags cybersäkerhet genom säkrare it-tjänster. Små och medelstora företag nyttjar stöd som erbjuds av organisationer såsom regionala handelskammare och bransch- och intresseorganisationer. Därtill ser aktörerna tillsammans över möjligheterna att nyttja gemensamma tekniska säkerhetslösningar vilket minskar små och medelstora företags behov att med egna resurser och kompetens omhänderta väsentliga områden för att cybersäkra sin verksamhet. EU:s kompetenscentrum för cybersäkerhet nyttjas genom att små och medelstora företag, via det nationella samordningscentret (NCC-SE), kan ansöka om medel för stärkt cybersäkerhetskapacitet.

4.2 Pelare B: Utvecklad kunskap och kompetens inom cybersäkerhet

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

Utöver aktiviteterna i handlingsplanen gäller följande övergripande resultatindikatorer för pelare B:

- 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.

4.2.1 Mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället

En tilltagande exponering för digitala hot och risker ställer krav på god cyberhygien och en medveten säkerhetskultur i hela samhället. Med cyberhygien avses grundläggande åtgärder för att skydda sig själv och andra online. Säkrare internetanvändning hos den enskilde bidrar till att Sveriges cybersäkerhet stärks genom att sårbarheten för bedrägerier och cyberangrepp minskar. Att åstadkomma beteendeförändringar hos allmänheten kräver kontinuerliga insatser från olika organisationer, såväl privata som offentliga och ideella.

Önskat läge 2030:
Medborgare är välinformerade om vikten av god cyberhygien och är bättre rustade för att hantera och möta cybersäkerhetsrisker. Åtgärder genomförs för att ge individer, utifrån deras förutsättningar och behov, bättre möjligheter till god cyberhygien. Arbetsgivare säkerställer också att processer och rutiner främjar säkra arbetssätt och cybersäkerhetsmedvetenhet. Statliga myndigheters informations- och utbildningskampanjer utvecklas löpande i syfte att få större genomslag och för att främja beteendeförändringar i samhället. Statliga myndigheter, ideella organisationer och företag bedriver i samarbete informations- och utbildningsinsatser inom cybersäkerhet för allmänheten. I detta beaktas skillnader i utsatthet för cybersäkerhetsrisker och skillnader i grundförutsättningar till god cyberhygien. Arbetet med att höja cybersäkerhetsmedvetenheten går hand i hand med insatser för att motstå hybridaktiviteter såsom stöd till medie- och informationskunnighet, bemötandet av desinformationskampanjer och Sveriges deltagande i det internationella arbetet med att stärka normer och regler för att värna det fria digitala informationsflödet. Exponering och ansvarsutkrävande av statliga cyberhotaktörer, inklusive inom utrikes- och säkerhetspolitiken, bidrar också till cybersäkerhetsmedvetenhet.

4.2.2 Mål 8: Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet

Kompetens inom cybersäkerhet blir allt viktigare och efterfrågan har länge varit större än utbudet. Utbildningsväsendet har en central roll i att möta samhällets behov genom att tillgodose grundläggande kunskaper i ämnet, väcka och stimulera intresse och ytterst stärka kompetensförsörjningen inom cybersäkerhet. Därtill behöver cybersäkerhetskompetensen hos

arbetsgivare och arbetstagare stärkas för att möta dagens och morgondagens behov inom cybersäkerhet. Befintlig kompetens behöver utvecklas och ny arbetskraft attraheras.

Önskat läge 2030:
Mer tillämpbara kunskaper i cybersäkerhet får genomslag i utbildningen i grundskolan, anpassade grundskolan, specialskolan och sameskolan. Elever i gymnasieskola, anpassad gymnasieskola och kommunal vuxenutbildning ges förutsättningar att förstå vikten av samhällets cybersäkerhet samt att få praktiska cybersäkerhetsfärdigheter. Både privata och offentliga organisationer bidrar fortsatt med interaktiva utbildningspaket och moduler som kan nyttjas för utbildning och fortbildning inom cybersäkerhet. Högskolor, universitet och yrkeshögskolor överväger om och hur cybersäkerhet bör införas i utbildningar. Därmed blir cybersäkerhet alltmer sammankopplat med alla ämnesområden.

Grundläggande och förutsättningsskapande utbildning för cybersäkerhet, såsom matematik, datavetenskap och kryptologi, står sig fortsatt stark. Interaktiva spel och tävlingar som vänder sig till ungdomar för att stimulera och väcka intresse för praktisk cybersäkerhet har bred spridning.

Cybercampus Sverige utgör ett nav för utbildning inom området och bidrar till förstärkt kompetensförsörjning av cybersäkerhetsexperter inom både offentlig och privat sektor. Organisationer såsom lärosäten, andra myndigheter och utbildningsanordnare inom yrkeshögskolan har tecknat avsiktsförklaringar att ingå i Cybercampus inom ramen för verksamheten. Statliga myndigheter verkar fortsatt för att väcka intresse för arbete inom cybersäkerhet. Berörda statliga myndigheter, kommuner och regioner samt andra organisationer har ett aktivt branschsamarbete om kompetensförsörjning inom cybersäkerhetsområdet och sprider kunskap om arbetsgivarnas nuvarande och framtida kompetensbehov. Nya målgrupper övervägs i större utsträckning för roller där avsaknad av tidigare erfarenhet eller utbildning inom området kan tillgodoses genom intensiv- och internutbildningar. Livslångt lärande och karriärbyte främjas, med omställningsstudiestödet eller liknande som en möjliggörare. Arbetsgivare säkerställer god fortbildning för anställda som arbetar med cybersäkerhet men också kompetensutveckling för andra medarbetare, chefer och ledning kring cybersäkerhet. Statliga myndigheter och privata organisationer erbjuder trainee-program inom cybersäkerhet i privat-offentlig samverkan. Därtill inspireras organisationer av, och utvärderar hur, lyckade satsningar i andra länder som rör kunskaps- och erfarenhetsutbyten kan omsättas till en svensk kontext.

4.2.3 Mål 9: Stärkt forskning och innovation på cybersäkerhetsområdet

I Sverige finns många världsledande teknikföretag, inklusive en expansiv cybersäkerhetsindustri innehållandes många innovativa små och medelstora företag som utvecklar och erbjuder konkurrenskraftiga cybersäkerhetslösningar. Traditionen av nära samarbete mellan staten,

lärosäten och industri finns även inom cybersäkerhetsområdet. Cybersäkerhetsforskning bedrivs vid flertalet universitet och högskolor vilka finansieras av såväl statliga som privata forskningsfinansiärer. Sverige har starka forskargrupper inom vissa av cybersäkerhetsforskningens områden men fältet är splittrat. En viktig faktor är att organisationer och företag ges goda förutsättningar för innovation, forskning och investeringar inom cybersäkerhetsområdet i Sverige. Nyttjandet av möjligheter och finansiering från bland annat EU:s program och fonder behöver öka.

Önskat läge 2030:
Sveriges forsknings- och teknikintensiva näringsliv inom cybersäkerhetsområdet ligger fortsatt i framkant och konkurrerar på en global marknad. Regeringens kraftfulla satsningar på forskning och innovation för banbrytande och strategisk teknik i den forsknings- och innovationspolitiska propositionen Forskning och innovation för framtid, nyfikenhet och nytta (prop. 2024/25:60) har även skapat goda förutsättningar för stärkt cybersäkerhetsforskning.

Satsningar som Cybercampus Sverige har stärkt forskning och innovation inom cybersäkerhet och bidrar till ett säkert digitaliserat och motståndskraftigt Sverige. Genom god samverkan med och mellan lärosäten och näringsliv fortsätter utvecklingen av funktioner såsom Cybercampus, Cybernoden och NCC-SE. Utvecklingen bidrar till ökad koordinering av cybersäkerhetsforskning och innovation samt goda förutsättningar för entreprenörskap på området. Forskning och innovation på cyberområdet har även en tvärvetenskaplig ansats och kommer därmed hela samhället till del genom att teknisk expertis alltmer sammanlänkas med andra ämnesområden. Forskningsresultat inom området leder i större utsträckning till innovation och kommersialisering. Statliga myndigheter bidrar aktivt till utveckling och kommersialisering av cybersäkerhetsinnovation genom exempelvis innovationsdrivande upphandling och stöttar organisationer att nyttja finansieringsmöjligheter för cybersäkerhet inom EU. Det finns en tillräckligt hög nivå av nationell medfinansiering för att säkra svenska aktörers aktiva och långsiktiga medverkan i fonder och program exempelvis inom cybersäkerhetsområdet. Sverige påverkar på ett tidigt stadium innehåll i arbetsprogram inför kommande utlysningar. Internationella forsknings- och innovationssamarbeten kring cybersäkerhet har ökat inom såväl EU och Nato som bilateralt med likasinnade länder.

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

Utvecklingen inom framväxande, banbrytande och strategiskt viktiga tekniker går snabbt. AI och kvantteknik är exempel på områden där omfattande framsteg har skett med relevans för cybersäkerhetsområdet. Ökad förmåga att hantera framväxande teknologier stärker både nationell säkerhet och konkurrenskraft. För att möta risker och möjligheter med framväxande teknologier behöver berörda organisationer prioritera

arbetet, och det är centralt med innovation och forskning av hög kvalitet inom teknikområden.

Utvecklingen inom kvantteknik, framför allt kvantdatorer, påverkar kryptografiska tekniker, vilket är ett väsentligt säkerhetsintresse och ett område där Sverige traditionellt legat i framkant. Organisationer har goda förutsättningar att skydda säkerhetsskyddsklassificerade uppgifter genom tillgång till godkända kryptografiska system som redan är kvantdatorsäkra, men fler insatser krävs för att bibehålla och utveckla förmågan samt för att kvantsäkra information som inte är säkerhetsskyddsklassificerad.

Teknikutveckling i stort, och kanske särskilt AI-utvecklingen, är ur många perspektiv fördelaktig men medför också ytterligare krav på cybersäkerhetsarbetet och på kontinuerlig utveckling av regelverk för att möta både möjligheter och utmaningar. Utvecklingen och implementeringen av säkra och etiska AI-system blir allt viktigare.

Önskat läge 2030:

Utvecklingen av AI nyttjas till en omfattande positiv påverkan på cybersäkerhetsområdet. Sverige har god tillgång till kompetens inom AI och är representerat i de internationella sammanhang där utveckling sker och kan därmed identifiera och hantera risker med AI, men också dra nytta av de möjligheter som AI innebär för cybersäkerhet.

Statliga myndigheter bibehåller en hög grad av kompetens, självförsörjning och nationellt oberoende i fråga om signalskydd. Utifrån antagandet om att kryptografiskt relevanta kvantdatorer kan komma att vara i bruk från början av 2030-talet, utvecklas och införs kvantsäkra kryptografiska funktioner i linje med de behov av koordinering och standardisering som följer av Sveriges EU- och Natomedlemskap. Kvantdatorsäkra kryptografiska lösningar prioriteras även för information som är känslig men inte säkerhetsskyddsklassificerad, såsom vissa affärshemligheter och personuppgifter. Berörda statliga myndigheter verkar för att kritiska krypteringstekniker och produkter även fortsättningsvis utvecklas i Sverige och anpassas för såväl nationella behov som behov inom EU och Nato. Svensk kryptoindustri och nya svenska företag på området har möjligheter att utvecklas i Sverige och leverera på en internationell marknad. Statliga myndigheter bidrar fortsatt till arbetet med kryptografiskt skydd inom EU och arbetet med att utveckla ett aktivt bidrag till Natos förmåga inom området, bland annat genom att skapa förutsättningar för att svenska kryptografiska produkter ska kunna användas inom alliansen. Regeringens kraftfulla satsningar på forskning och innovation för banbrytande och strategisk teknik i den forsknings- och innovationspolitiska propositionen Forskning och innovation för framtid, nyfikenhet och nytta (prop. 2024/25:60) har ökat den långsiktiga kompetensförsörjningen inom olika teknikområden, vilket är av stor betydelse för såväl svensk konkurrenskraft och samhällsutveckling som cybersäkerhet.

4.3 Pelare C: Förmåga att förhindra och hantera cybersäkerhetsincidenter

Pelaren *Förmåga att förhindra och hantera cybersäkerhetsincidenter* 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.

Utöver aktiviteterna i handlingsplanen gäller följande övergripande resultatindikatorer för pelare C:

- 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 incidentrapportering till organisationer som rapporterar incidenter har förbättrats.

4.3.1 Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt

Att kontinuerligt kartlägga, identifiera och bedöma cyberhot på hela skalan kräver ofta omfattande samarbete mellan nationella myndigheter och med myndigheter i andra stater, inte minst genom etablerade samarbeten inom EU och Nato. Samarbete med näringsliv och ideella organisationer ger också viktiga bidrag. Organisationers olika informationsflöden kan innehålla viktig information både för den egna organisationen och för andra när det gäller cybersäkerhetsincidenter, sårbarheter och hot. Ett välfungerande samarbete med hög tillit aktörerna emellan lägger därför grunden för informationsdelning och varningar om relevanta hot och sårbarheter, men också för att utreda och attribuera angrepp.

Önskat läge 2030:
NIS 2-direktivets och cyberresiliensförordningens krav om samordnad delgivning av information om sårbarheter bidrar till ökad informationsdelning om sårbarheter som upptäcks i produkter och tjänster. NCSC har väletablerade metoder för internationellt och privat-offentligt samarbete. Positiva exempel inom privat-offentlig samverkan har vidareutvecklats. Plattformar för att dela säkerhetsrelaterad information etableras, både inom och mellan offentlig och privat sektor, som möjliggör ökad delning och analys av realtidsinformation på teknisk och operativ

nivå. Genom ökad analys av sådan information stimuleras även organisationers möjlighet att implementera, och dela med sig av förslag på, relevanta säkerhetshöjande åtgärder. Arbetet bidrar också till utvecklade och ändamålsenliga lägesbilder från NCSC till gagn för olika målgrupper samt vidareutvecklad samverkan mellan relevanta myndigheter om attribueringsfrågor. Informationsdelning sker, utifrån lagstiftning och etablerade processer, till gagn för alla inblandade parter och stärker bland annat förmågan att identifiera, hantera och utreda incidenter och angrepp.

Ett utökat internationellt samarbete på cyberområdet bidrar till värdefulla lärdomar om bland annat informationsdelningsmetoder som anpassas till svensk kontext. Privat-offentlig samverkan bidrar till ökad förmåga att upptäcka och motstå cyberangrepp vare sig de utgör en enskild händelse eller en del av en hybridaktivitet.

4.3.2 Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter

En effektiv samordning är av central betydelse vid cybersäkerhetsincidenter. Lärdomar och erfarenheter behöver få genomslag i utvecklingen av nationell incidenthanteringsförmåga. Anmälnings- och rapporteringsbenägenheten vid incidenter behöver stimuleras, samtidigt som utmaningarna med överlappande rapporteringskrav behöver hanteras. För att effektivt nyttja de samlade utredande och förebyggande resurserna på cybersäkerhetsområdet behöver också myndigheters informationsdelning om incidenter vara ändamålsenlig. Sveriges förmåga att identifiera, hantera och bemöta cybersäkerhetsincidenter ska stärkas.

Önskat läge 2030:

Statliga myndigheter utvecklar kontinuerligt den nationella operativa förmågan för stöd och hantering vid cybersäkerhetsincidenter. NCSC utvecklar och stärker Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter. Privat-offentligt samarbete kring cybersäkerhetsincidenter har utvecklats och nyttjar den incidenthanteringskompetens som finns i privat sektor. Organisationer inom berörda sektorer har NCSC som kontaktpunkt vid hantering av cybersäkerhetsincidenter[2]. Regelbundna incidentövningar sker inom och mellan organisationer. Nationell övningsverksamhet fortsätter bedrivas och utvecklas. Statliga myndigheter har etablerat gemensamma plattformar för incidentrapportering vilket underlättar för organisationer både att utföra sin rapporteringsplikt och att få återkoppling och stöd samtidigt som ökad informationsdelning mellan relevanta myndigheter förenklas. Statliga myndigheters kommunikation om förmågehöjande åtgärder relaterat till sannolikhet eller konsekvens för en incident sker löpande. Kommunikation mellan mottagande statliga myndigheter och drabbade organisationer, under och efter att en

[2] Detta gäller dock inte för exempelvis säkerhetshotande händelser enligt säkerhetsskyddsförordningen.

cybersäkerhetsincident inträffat, utvecklas. Organisationers rapporterings- och anmälningsbenägenhet vid cybersäkerhetsincidenter ökar.

Sverige har också aktivt deltagit i samordnad hantering av storskaliga cybersäkerhetsincidenter inom ramen för samarbetsförfaranden på EU-nivå och bidragit till ett effektivt gränsöverskridande samarbete på operativ nivå mellan medlemsstaterna.

4.3.3 Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott

Cyberbrott utvecklas ständigt och genererar stora brottsvinster. Detta medför utmaningar för rättsvårdande myndigheter och ett behov av kontinuerligt utvecklingsarbete för att möta nya utmaningar. Den ökande andelen brott med digitala element belyser kopplingen mellan cybersäkerhetsarbetet och bekämpningen av cyberbrottslighet, där stärkt cybersäkerhet leder till färre cyberbrott. Detta understryker vikten av att brottsbekämpande myndigheter behöver öka sina förmågor att utreda och lagföra digitala brott.

Anmälningsbenägenheten till brottsbekämpande myndigheter behöver också öka. Mängden cyberangrepp mot svensk, digital kritisk infrastruktur eller enskilda personer från utlandet visar att det är viktigt att Sverige deltar aktivt i internationella samarbeten som syftar till att bekämpa ransomware-angrepp och datastölder.

Önskat läge 2030:

Brottsbekämpande myndigheters utveckling av specialistfunktioner för cyberbrottslighet har inneburit en förbättrad förmåga att bekämpa denna brottslighet. Samarbetet mellan NCSC och brottsbekämpande myndigheters specialistfunktioner har bidragit till bättre lägesbilder. De brottsbekämpande myndigheternas förmåga att inhämta information i digitala system och från kommunikationstjänster har utvecklats. Därtill har lagstiftningen utvecklats, bland annat genom EU:s förordning om europeiska bevarande- och utlämnandeorder för elektroniska bevis. Bekämpningen av den kriminella ekonomin har förstärkts och brottsvinsterna från cyberbrott har minskat.

Statliga myndigheters kompetensförsörjning när det gäller digital brottsbekämpningsförmåga har stärkts och kunskapen om kriminella aktörers tillvägagångssätt och effekter av motåtgärder har ökat. De operativa samarbetsmöjligheter som erbjuds av Eurojust och Europol har förstärkts och nyttjas i större omfattning.

Berörda statliga myndigheters stöd och rådgivning om hantering och förebyggande av cyberbrottslighet har ökat. Brottsförebyggande samarbeten mellan ideell sektor, näringslivet och statliga myndigheter har vidareutvecklats. Mörkertalen för rapporterade digitala brott har minskat och närmar sig i vart fall rapporteringsgraden för fysiska brott.

En ökad förmåga att bekämpa cyberbrott har bidragit till en ökad trygghet för individer och organisationer i Sverige samt, givet att statliga hotaktörer kan använda kriminella grupper som mellanhänder för olika former av hybridaktiviteter, till att Sveriges samlade förmåga att motstå hybridhot har förstärkts.

5 Genomförande och uppföljning

Den nationella strategin för cybersäkerhet ger inriktningen för regeringens arbete med frågor av betydelse för Sveriges cybersäkerhet. Strategin kommer regelbundet och minst vart femte år att utvärderas på grundval av strategins resultatindikatorer i enlighet med NIS 2-direktivets krav.

Av bilagd handlingsplan framgår att strategin kommer att omsättas i konkret handling bland annat genom specifika uppdrag och styrning av myndigheter. Det kan också krävas andra regeringsbeslut för att genomföra strategin i denna del. Teknik- och hotutvecklingen innebär att cybersäkerhetsområdet förändras och utvecklas i snabb takt och det krävs därför flexibilitet i genomförandet av strategin. Handlingsplanens innehåll kommer därför att uppdateras löpande. Därutöver kommer utvärdering och revidering av handlingsplanens innehåll att ske på det sätt som regeringen ser behov av. Bilagan som gäller organisationer med roller och ansvarsområden inom cybersäkerhet kommer också att behöva uppdateras, bland annat när den nationella regleringen som genomför NIS 2-direktivet i Sverige har trätt i kraft. Denna uppdatering kommer att ske på det sätt och i den form som regeringen ser behov av.

6 Översikt över utmaningar och mål

Följande tabell visar förhållandet mellan utmaningarna i cybersäkerhetslandskapet i avsnitt 4 och målen i avsnitt 5.

Utmaning:	**Mål som huvudsakligen omhändertar utmaningen:**
4.1 Hot från statliga aktörer	Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering Mål 3: Stärkt säkerhetsarbete inom kritisk infrastruktur Mål 4: Robustare digitala leveranskedjor och minskat beroende Mål 10: Stärkt förmåga att hanteraframväxande teknologiers risker och möjligheter Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott

4.2 Hot från cyberaktivister	Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering Mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott
4.3 Hot från cyberbrottslighet och kriminella grupperingar	Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete Mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället Mål 10: Stärkt förmåga att hantera framväxande teknologiers risker och möjligheter Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott
4.4 Brister i cybersäkerhetsarbetet	Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering Mål 4: Robustare digitala leveranskedjor och minskat beroende Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete Mål 8: Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet
4.5 Komplex reglering	Mål 5: Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete
4.6 Kompetens- och kunskapsbrist	Mål 7: Ökad cybersäkerhetsmedvetenhet och cyberhygien i samhället Mål 8: Stärkt kompetensförsörjning, utbildning och fortbildning inom cybersäkerhet Mål 9: Stärkt forskning och innovation på cybersäkerhetsområdet
4.7 Bristande incidenthantering	Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering

	Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott
4.8 Outvecklad privat-offentlig informationsdelning	Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter Mål 13: Utvecklad förmåga att förebygga och bekämpa cyberbrott
4.9 Sårbara leveranskedjor, beroenden och produkter	Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering Mål 4: Robustare digitala leveranskedjor och minskat beroende Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete Mål 11: Effektivare informationsdelning nationellt och internationellt Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter
4.10 Utmaningar kopplat till utvecklingen i digital infrastruktur och digitala tjänster	Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer Mål 2: Stärkt cybersäkerhet i statlig och kommunal förvaltnings informationshantering Mål 3: Stärkt säkerhetsarbete inom kritisk infrastruktur Mål 4: Robustare digitala leveranskedjor och minskat beroende Mål 5: Förenklad regelefterlevnad och stärkt funktionellt tillsynsarbete Mål 6: Utvecklat stöd för små och medelstora företags cybersäkerhetsarbete Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter
4.11 Utmaningar med uppkoppling av enheter och infrastruktur	Mål 1: Ökat cybersäkerhetsarbete hos privata och offentliga organisationer Mål 3: Stärkt säkerhetsarbete inom kritisk infrastruktur

	Mål 4: Robustare digitala leveranskedjor och minskat beroende. Mål 11: Effektivare och säkrare informationsdelning nationellt och internationellt Mål 12: Stärkt privat-offentlig hantering av cybersäkerhetsincidenter
4.12 Teknikutvecklingen	Mål 4: Robustare digitala leveranskedjor och minskat beroende Mål 10: Stärkt förmåga att hantera framväxande teknologiers risker och möjligheter

7 Begreppsförteckning

Allriskperspektiv: Används i denna strategi på motsvarande sätt som allriskansats i skäl 79 i NIS 2-direktivet.

Cyberresiliensförordningen: Förordningen innebär bland annat att vissa kritiska produkter och tjänster omfattas av högre säkerhetskrav (bland annat bedömning av överensstämmelse samt tredjepartsgranskning enligt EU:s New Legal Framework och CSA:s ramverk för cybersäkerhetscertifiering).

Cybersäkerhetsakten: Akten reglerar bland annat cybersäkerhetscertifiering på den inre marknaden som möjliggör att olika it-produkter och it-tjänster (till exempel molntjänster) kan certifieras mot en ensad, kvalitetssäkrad och gemensam uppsättning krav. Sådan certifiering kan bland annat användas vid myndigheters kravställning i samband med upphandling, som krav i tillsyns- och sektorsmyndigheters föreskrifter eller för att visa uppfyllnad av olika cybersäkerhetskrav vid myndighetstillsyn.

Cyber range: Testbädd och övningsanläggning för cybersäkerhet.

Cyberangrepp: En interaktion mellan en angripare och ett mål som i) angriparen inte har rätt att utföra mot målet, ii) medför ett utbyte av information som resulterar i en interaktion, konfigurering, installation/sparande, avinstallation/raderande eller överbelastning i något av målets informationssystem, iii) resulterar i minst en för målet oönskad konsekvens i termer av konfidentialitet, riktighet eller tillgänglighet för målet eller för andra via målet och vi) som angriparen utför i ett antagonistiskt syfte.

Cybersäkerhet: Används i denna strategi i enlighet med NIS 2-direktivet, som nyttjar cybersäkerhetsaktens definition (all verksamhet som är nödvändig för att skydda nätverks- och informationssystem, användare av dessa system och andra berörda personer mot cyberhot).

Digital leveranskedja: Tjänster och infrastruktur som levererar eller möjliggör leverans av digitala produkter vilka används för att upprätta, upprätthålla, utveckla eller återställa en verksamhets informationshantering och informationssystem.

IoT: Internet of Things, eller Sakernas internet, rör användandet av uppkopplade föremål i verksamheter.

Konfidentialitet: En aspekt av cybersäkerhet som innebär att endast behöriga kan ta del av informationen. Frågor som rör offentlighetsprincipen och allmänhetens tillgång till handlingar faller dock utanför denna definition.

Monoberoende: Tjänster eller infrastruktur som organisationer är beroende av och där alternativ saknas om den aktuella tjänsten eller infrastrukturen skulle upphöra.

NIS 2-direktivet: 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).

Nätverks- och informationssystem: ett nätverks- och informationssystem enligt definitionen i artikel 4.1 i direktiv (EU) 2016/1148.

Ransomware: Utpressningsvirus och program som krypterar hela eller delar av en verksamhetsinformation som lagras på drabbade informationssystem och gör informationen otillgänglig. Syftar till att försöka utpressa en organisation eller individ på en lösensumma. Angrepp kan även genomföras i syfte att nå specifik information, till exempel för underrättelseinhämtning.

Riktighet: En aspekt av cybersäkerhet som innebär att information och informationssystem är korrekta eller fungerar korrekt och inte ändras på ett felaktigt sätt.

Systematisk cybersäkerhet: Förebyggande och kontinuerlig anpassning av skydd utifrån behov och risker. Det innefattar arbetssätt baserat på en metodik för verksamhetsrisk, som syftar till att upprätta, införa, driva, övervaka, granska, underhålla och förbättra organisationens informationssäkerhet, det vill säga skydd av informationstillgångar som gäller konfidentialitet, riktighet och tillgänglighet.

Tillgänglighet: Tillgänglighet är aspekten att information eller informationssystem ska finnas tillgängligt när de behövs.

Överbelastningsangrepp: Angreppsmetod som bygger på att stora mängder datatrafik eller förfrågningar skickas mot en server eller annan nätverkskomponent i syfte att begränsa dess förmåga att bearbeta data och därmed blockera åtkomst för annan, legitim datatrafik.

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 cybersäkerhetsarbetet är under översyn och kan komma att påverka ansvarig(a) myndigheter 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 cybersäkerhetsmedvetenhetenen 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.

Organisationer med roller och ansvarsområden inom cybersäkerhet

Cybersäkerhet är en horisontell fråga och medför ett sektoröverskridande ansvar inom regeringen och Regeringskansliet.

Denna bilaga kommer uppdateras när NIS 2-direktivet implementerats nationellt och ansvarsförhållanden har definierats samt när uppdrag att lämna förslag på organisationsförändring och ansvarsfördelning för samhällets informations- och cybersäkerhet (dir. 2024:111) redovisats och omhändertagits.

Nationellt cybersäkerhetscenter (NCSC)

Nationellt cybersäkerhetscenter har i uppdrag att utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.

Från och med den 1 november 2024 finns centret inom FRA som har ansvaret för att leda NCSC.

Gemensam kontaktpunkt

Den roll som enligt NIS 2-direktivet benämns *gemensam kontaktpunkt* (på engelska SPOC, Single Point Of Contact*)* kommer att utses och närmare definieras i kommande reglering som implementerar NIS 2-direktivet i Sverige. Den gemensamma kontaktpunkten ska enligt NIS 2-direktivet utöva en sambandsfunktion som säkerställer ett gränsöverskridande samarbete mellan medlemsstatens myndigheter och relevanta myndigheter i andra medlemsstater och, när det är lämpligt, kommissionen och Enisa samt ett sektorsövergripande samarbete med andra behöriga myndigheter i medlemsstaten.

För NIS-direktivet har MSB uppgiften att vara *nationell gemensam kontaktpunkt*[1].

[1] Uppgiften inkluderar bland annat att tillhandahålla vägledning och utbyta praxis i fråga om NIS-direktivets genomförande, samverkan med regulatoriska policyfrågor, tillsynssamordning, stödja samordning mellan NIS 2- och CER-direktiven, säkerställa samarbete mellan brottsbekämpande myndigheter och dataskyddsmyndigheter, förvalta och utveckla föreskrifter om informations- och cybersäkerhet för aktörer som omfattas av NIS-regleringen.

Nationell CSIRT-enhet

CERT-SE är nationell CSIRT-enhet enligt NIS-direktivet, vilket regleras i förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Varje medlemsstat ska i enlighet med NIS 2-direktivet utse eller inrätta en eller flera CSIRT-enheter (på engelska Computer Security Incident Response Team). CSIRT-enheten ska enligt NIS 2-direktivet bland annat övervaka och analysera cyberhot, sårbarheter och incidenter på nationell nivå samt tillhandahålla varningar och sprida information om dessa. Sveriges nationella CSIRT-funktion kommer att pekas ut i kommande reglering som implementerar NIS 2-direktivet i Sverige.

Cyberkrishanteringsmyndighet

Varje medlemsstat ska i enlighet med NIS 2-direktivet utse eller inrätta en eller flera cyberkrishanteringsmyndigheter med ansvar för hanteringen av storskaliga cybersäkerhetsincidenter och kriser.[2]

Ansvarig cyberkrishanteringsmyndighet kommer att utses av regeringen.

Statliga myndigheter som tar emot incidentrapporter[3]

Vid en cybersäkerhetsincident finns ett antal aktörer som, beroende på typ av incident, ska ta emot rapporter om incidenter utifrån olika regleringar. Några av dessa är:

- CERT-SE är mottagare av it-incidentrapporter, vilket följer av ett flertal regleringar.
- Säkerhetspolisen tar emot anmälningar om säkerhetshotande händelser och verksamhet enligt säkerhetsskyddsförordningen (2021:955). Om verksamhetsutövaren tillhör Försvarsmaktens tillsynsområde ska anmälan också göras till Försvarsmakten.
- Integritetsskyddsmyndigheten hanterar personuppgiftsincidenter.
- Polismyndigheten tar emot anmälningar om misstänkta brott[4].

[2] Varje medlemsstat ska anta en nationell plan för hanteringen av storskaliga cybersäkerhetsincidenter och kriser. Planen ska bland annat innehålla cyberkrishanteringsmyndighetens uppgifter och ansvarsområden. Utformningen av den nationella planen ingår inte i utredningens uppdrag.

[3] Detta avsnitt berör inte statliga myndigheter som mottar sektorspecifik incidentrapportering såsom för elektroniska kommunikationer eller inom exempelvis finanssektorn.

[4] Incidenter som rapporteras under olika regelverk bör alltid polisanmälas av organisationer om incidenterna misstänks bero på brott. Myndigheter som tar emot incidentrapportering har också rutiner för att vid behov notifiera Polismyndigheten.

Tillsynsmyndigheter under NIS-regleringen

Sex tillsynsmyndigheter ansvarar för tillsynen inom de sektorer som träffas av NIS-direktivet. MSB driver ett nationellt samarbetsforum gällande NIS-frågor där de sex tillsynsmyndigheterna och Socialstyrelsen ingår. Forumets syfte är att underlätta den nationella samordningen och att åstadkomma en effektiv och likvärdig tillsyn. De sex NIS-tillsynsmyndigheterna är följande.

Tillsynsmyndighet	**Sektor**
Statens energimyndighet	Energi
Transportstyrelsen	Transport
Finansinspektionen	Bankverksamhet Finansmarknadsinfrastruktur
Inspektionen för vård och omsorg	Hälso- och sjukvård
Livsmedelsverket	Leverans och distribution av dricksvatten
Post- och telestyrelsen	Digital infrastruktur

NIS 2-direktivet omfattar 18 sektorer. Tillsynsansvaret, som föreslås fördelas över flera myndigheter, kommer att framgå i kommande nationell författning som implementerar NIS 2-direktivet i Sverige.

Utöver NIS-regleringen finns flera andra relevanta regelverk med cybersäkerhetskrav och som omfattas av tillsyn. Dessa berörs inte närmare i denna strategi.

Cybersäkerhet i det civila försvaret

Beredskapsmyndigheterna ansvarar, enligt förordningen (2022:524) om statliga myndigheters beredskap, för att egna informationshanteringssystem uppfyller sådana grundläggande och särskilda säkerhetskrav att myndighetens verksamhet kan utföras på ett tillfredsställande sätt.

Myndigheter med särskilt ansvar för säkerhetsskydd

Säkerhetspolisen och Försvarsmakten har enligt säkerhetsskyddsförordningen till uppgift att samordna övriga tillsynsmyndigheter inom säkerhetsskyddsområdet och utövar även tillsyn över de allra mest skyddsvärda verksamheterna.

Försvarsmakten leder och samordnar totalförsvarets signalskyddstjänst. Myndigheten ansvarar bland annat även för att godkänna kryptografiska funktioner för skydd av säkerhetsskyddsklassificerade uppgifter samt för att meddela föreskrifter inom dessa områden.

Enligt säkerhetsskyddslagen (2018:585) ska informationssäkerhet förebygga att säkerhetsskyddsklassificerade uppgifter röjs, ändras, görs otillgängliga eller förstörs av obehöriga. Utöver det ska informationssäkerhet också förebygga skadlig inverkan i övrigt på

uppgifter och informationssystem som gäller säkerhetskänslig verksamhet. Med ”säkerhetsskyddsklassificerade uppgifter” avses uppgifter som rör säkerhetskänslig verksamhet och som därför omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400), eller som skulle ha omfattats av lagen om den varit tillämplig i den aktuella verksamheten.

Nationell myndighet för cybersäkerhetscertifiering

Försvarets materielverks (FMV) är nationell myndighet för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt. FMV bedriver tillsyn och samverkan över det europeiska ramverket för cybersäkerhetscertifiering enligt EU:s cybersäkerhetsakt.

Kommuner och regioner

Av 14 kap. 2 § regeringsformen framgår att kommunerna sköter lokala och regionala angelägenheter av allmänt intresse på den kommunala självstyrelsens grund. Närmare bestämmelser om detta finns i lag. På samma grund sköter kommunerna även de övriga angelägenheter som bestäms i lag. Kommuner och regioner ansvarar för sin egen cybersäkerhet och har en central roll för Sveriges cybersäkerhet.

Andra nationella cybersäkerhetsaktörer

Centrum för cyberförsvar och informationssäkerhet (CDIS)

CDIS initierades genom ett nära samarbete mellan Kungl. Tekniska högskolan (KTH) och Försvarsmakten. Totalförsvarets forskningsinstitut (FOI), MSB, FRA och Försvarshögskolan ingår också i CDIS. CDIS är en del av Skolan för elektroteknik och datavetenskap vid KTH.

En styrgrupp med partnerrepresentanter leder centrets arbete.

Cyber Range and Training Environment (Crate)

FOI, Försvarsmakten och MSB har i samverkan utvecklat Sveriges nationella cyberanläggning för totalförsvaret, Crate. FOI använder sedan 2009 Crate för att tillhandahålla träning i cybersäkerhet till relevanta aktörer inom totalförsvaret.

RISE Cyber Range

RISE Cyber Range är en testbädd som drivs av RISE (Research Institutes of Sweden). Genom testbädden kan företag och organisationer testa tekniska system, identifiera sårbarheter och säkerställa adekvata rutiner och organisation. Målgruppen är både näringsliv som offentlig sektor.

Cybercampus Sverige

Cybercampus Sverige inrättades 2024 och har fokus på forskning, innovationer och utbildningar. Det är en satsning och ett samarbete mellan universitet, institut, myndigheter och företag i hela Sverige. KTH är huvudman för uppdraget att etablera och utveckla Cybercampus Sverige.

Cybernoden

Cybernodens primära syfte är att skapa en samverkansplattform. Cybernoden utgör den nationella kompetensgemenskapen för forskning och innovation inom cybersäkerhet och drivs av RISE på uppdrag av NCC-SE, inom ramen för EU:s kompetenscentrum för cybersäkerhet.

Nationellt it-brottscentrum

Nationellt it-brottscentrum, utgör Polismyndighetens expertfunktion för utredning av komplexa cyberbrott, internetrelaterade sexualbrott mot barn och andra brott där internet är en bärande del. Sektionen biträder även den övriga brottsbekämpande verksamheten med insamling och hantering av digital bevisning och digitala spår.

NCC-SE

NCC-SE är Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet. NCC-SE främjar samarbete mellan svenska och europeiska forskare, företag och myndigheter för utveckling av cybersäkerhetslösningar.

NCC-SE bidrar i framtagande av arbetsprogram på EU-nivå, marknadsför de europeiska cybersäkerhetsutlysningarna samt ger vägledning till svenska aktörer som söker EU-medel för projekt inom arbetsprogrammen. NCC-SE stödjer, tillsammans med övriga medlemsländers nationella samordningscenter, EU:s kompetenscentrum för cybersäkerhet (ECCC) i uppdraget för ökad cybersäkerhet inom EU.

Försvarsdepartementet

Utdrag ur protokoll vid regeringssammanträde den 20 mars 2025

Närvarande: statsrådet Busch, ordförande, och statsråden Svantesson, Ankarberg Johansson, Edholm, J Pehrson, Waltersson Grönvall, Jonson, Strömmer, Forssmed, Tenje, Slottner, Malmer Stenergard, Kullgren, Liljestrand, Brandberg, Bohlin, Carlson, Pourmokhtari

Föredragande: statsrådet Bohlin

Regeringen beslutar skrivelse Nationell strategi för cybersäkerhet 2025–2029